Threat Highlight Report

February 2023

WITH secure

Contents

Foreword

WithSecure's monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, providing an overview of this month's cybersecurity news, the changing threat landscape and relevant advice.

This month we look at the abuse of Microsoft's OneNote, ongoing "hacktivist" activity, and ongoing campaigns by Callisto (Russia) and TA453 (Iranian) using social engineering and spear phising.

We look at the ransomware landscape, including the most prevalent hack/leak actors from February, the ESXiArgs campaign which has devasted vulnerable ESXi instances, the potential end of Hive, Alphv's attack on an Irish University and we examine newcomers Nevada and Mimic.

We also discuss the exploitation of GoAnywhere and ManageEngine, as well as problems with KeePass, Chromebooks, and the targeting of gambling companies and a new QR code phishing technique.

Included in our research section are links to reports by WithSecure™ fellows on **Detecting OneNote Abuse and Analysis of YouTube USDT crypto scams**.

As ever, we look to WithSecure's telemetry for insight into the top vulnerabilities exploited in the wild as seen by WithSecure™ and CISA's telemetry.

- Ziggy Davies, Threat Intelligence Analyst

1 Monthly highlights

1.1 OneNote abuse

Back in August 2022 the researcher Emeric Nasi published research on the potential for the Microsoft Office note-taking product OneNote to be leveraged by penetration testers/ hackers. The findings of that research suggested:

- “(OneNote) Is not affected by Protected View/ MOTW
- Allows embedding Malicious Excel/Word/PPT files that will be played without protected view
- Allows embedding HTA, LNK, EXE files and spoof extensions
- Allows formatting document in a way user are tricked into opening a malicious file or a link
- Can be automated using OneNote.Application and XML
- Is supported by BallisKit MacroPack Pro tool”

Thankfully, the ability to abuse OneNote to bypass Mark of the Web (MOTW) protections was silently patched in January, however, there are still a number of potential issues with OneNote. Many organizations have noted an uptick in OneNote adoption by threat actors, and have released related research, including fellows at WithSecure™:

- Detecting OneNote Abuse - WithSecure™
- OneNote documents Increasingly Used to Deliver Malware - Proofpoint
- OneNote Malware – Marco Ramilli

WithSecure™ Insight

Threat actors often seek to diversify their tactics, techniques, and procedures, especially since the introduction of MOTW, blocking of macros, and better user education surrounding phishing. The adoption of delivering OneNote files (.one and .onepkg) is part of this trend of threat actors seeking to get ahead of the curve.

The abuse of OneNote by threat actors is discussed further in the “research” section of this Threat Highlight Report, containing a summary of the findings by WithSecure™ fellows Riccardo Ancarani and Jojo O’Gorman in their research.

What can you do?

WithSecure’s fellows recommend the following mitigations:

- If possible, block direct download of .one and .onepkg files at the proxy level
- If possible, block .one and .onepkg mail attachments
- Monitor the operations of the OneNote.exe process, especially when a .one file is downloaded from the internet
- Pay particular attention to process creation events associated with common LOLBins
- File write operations should also be monitored closely

1.2 Ongoing “hacktivist” activity

We have reported on pro-Russian and Russian-backed hacktivist groups on multiple occasions since the invasion of Ukraine, and this activity continues to go on and has developed into a constant issue.

This month the so-called hacktivist group **Anonymous Sudan** has been heavily targeting Sweden and Swedish entities, including the railways and an airline. While this group represents itself as acting in response to recent protest activity in Sweden, a look at the group’s Telegram history and infrastructure shows the group is aligned with Russia and has no connection with Sudan or a former Anonymous Sudan campaign from 2019, it is almost certainly a thinly veiled ruse for pro-Russian activity.

In addition to the above activity, **KillNet** has been targeting US healthcare organizations, as well as organizations in other NATO nations, with the group offering access to their **Passion** botnet.

WithSecure™ Insight

While most threat actors carry out attacks for the purpose of gain, whether that be financial or in the interests of their nation, hacktivists carry out their attacks due to a political agenda or in response to a perceived injustice. An example of this is the hacktivist collective Anonymous, which often responds to perceived social injustices. However, we have seen a different type of hacktivist since the invasion of Ukraine, those who carry out attacks in patriot support of their nation during a time of war. There has also been assessment exploring the extent to which Russian state has influence over these pro-Russia hacktivist groupings. This is explored in September’s WithSecure™ Threat Highlight Report.

This activity is ongoing, and a handful of pro-Russian groups have become prevalent, who don’t only target Ukraine but also Ukraine’s allies and members of NATO, primarily with orchestrated DDoS attacks. Two of the main groups are **KillNet** and **NoName057(16)**, though recently they have been joined by **Anonymous Sudan**, who despite their name and rhetoric are clearly aligned with the interests of Russia, rather than Anonymous and/or Sudan.

A recent announcement in Russia suggests that hackers acting in the interests of the nation will not be pursued or prosecuted, ultimatley making all hostile foreign entities fair game. This, of course, is nothing new, as Russia has historically taken a relaxed stance regarding prosecution of cyber criminals operating within their borders yet targeting western organisations, and this statement just ratifies that fact.

It is easy to look at these hacktivist groups as a nuisance as DDoS attacks are disruptive rather than destructive, but impact to organisations in the firing line is being observed and shouldn’t be disregarded.

What can you do?

DDoS protections are reliant upon the use of specially configured network equipment or cloud-based protection services, offered by DDoS specialists. Work by Team Cymru has noted that the DDoS activity orchestrated by these groups originates from a narrow netblock, suggesting it could be resolved through filtering, though this is always a problematic approach due to the risk of blocking legitimate activity.

Monitoring of these groups is also useful as many of their attacks are discussed and advertised ahead of time (albeit at short notice) via their public Telegram channels, giving defenders the opportunity to pre-empt potential attacks.

1.3 Russia & Iran using social engineering

The UK National Cyber Security Centre (NCSC) have reported on two separate, but similar, spear phishing campaigns being conducted by the Russian threat actor **Callisto** (SEABORGIUM) and Iranian **TA453** (Charming Kitten).

The report states that both groups are targeting the following sectors/persons:

- Education
- Defense
- Government
- Non-governmental organizations
- Think-tanks
- Politicians
- Journalists, and
- Activists

WithSecure™ Insight

These campaigns are noteworthy, as both **Callisto** and **TA453**, are apparently using very similar TTPs, despite being entirely unconnected, and are both using social engineering to increase the likelihood of target interaction.

Social engineering is becoming far more commonplace, likely due to threat actors realizing that mass spam phishing is failing to gain the same victim interaction that it once did, thanks to better security practices and user education. In these incidents, social engineering involves:

- Reconnaissance to identify suitable targets within organizations, often conducted using social media
- Contacting targets and attempting to build rapport, often by discussing topics that would seem legitimate to the target
- Delivery of malicious links designed to capture credentials, by:
  - Typical phishing links
  - Embedded malicious links within benign documents
  - Malicious links imitating Zoom meeting links
  - Malicious links delivered via the chat capability within a video meeting

What can you do?

The NCSC are recommending the following mitigations, which we fully agree with:

- Use strong passwords
- Use multi-factor authentication (MFA), and if possible those which cannot be bypassed through MFA fatigue, sim-swapping or social engineering.
- Exercise vigilance, and be wary of unsolicited contact from any person, especially if they are asking to exchange correspondence via your personal email address

2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion ransomware leak sites which are parsable and was captured between 24th January 2023 and 21st February 2023.

There has been a 92% increase on last month's activity.

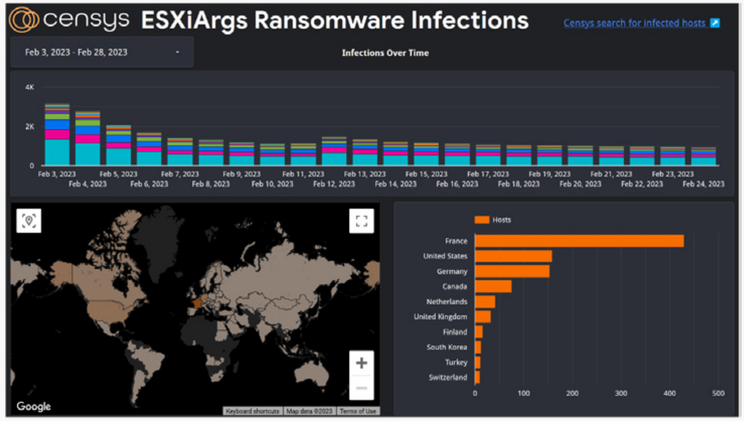
Group	Victims	Percentage
LockBit	120	52%
Alphv (BlackCat)	24	10%
Clop	19	8%
BianLian	18	8%
Royal	17	7%
Play	12	5%
ViceSociety	10	4%
Mallox	6	3%
RansomHouse	3	1%
0mega	1	<1%
Daixin	1	<1%
Qilin	1	<1%

2.1 ESXiArgs

Since the 3rd of February, a new ransomware variant dubbed **ESXiArgs** has been used to target vulnerable ESXi systems, which are internet-facing, or part of previously compromised networks.

ESXi is very popular, and unfortunately the threat actors in this campaign are using old, but apparently often unpatched vulnerabilities to gain access, mainly CVE-2021-21974 a heap-overflow vulnerability that can result in remote code executed (RCE).

The attack surface identification company Censys have built a dashboard to track **ESXiArgs** infections, with several thousand systems being potentially impacted.



As you can see, the majority of infections have occurred on hosts located in France, the United States, Germany, Canada and the Netherlands.

This campaign once again highlights the importance of patch management, as the vulnerabilities being exploited are all fairly old and have been fixable with patches from VMware. VMware have released a Q&A on the topic and CISA have released a decryption tool that *may* help some victims recover their data, but it's important to note that the attacker has reportedly modified their attack to negate the tools effectiveness. This story serves as yet another reminder of the importance of effective attack surface monitoring, and in the agility and ability of ransomware actors to respond to disruption efforts.

2.2 The end of Hive???

Hive ransomware (aka HiveLeaks) have been a menace since about December 2021, and since that time have leaked data from 207 different organizations on their leaksite. The group hadn't been posting since early January, and we perhaps now know why…they were hacked by the FBI.

The FBI reportedly breached **Hive's** infrastructure and has been extracting decryption keys for victims, so that they can recover their data for free, apparently saving victims around $130 million in potential ransom payments. The FBI has hopefully ended **Hive's** criminal career, delivering a death blow to their leak site by seizing it.

Unfortunately, history teaches us that ransomware groups are very hard to outright erradicate, and only time will tell whether the criminals behind **Hive** will return, whether that be under the **Hive** name, or like many others have, under a new moniker. We do assess that offensive repercussions from responsible authorities is an effective deterrent to some ransomware activity.

2.3 Alphv attack on Munster Technological University

The Munster Technological University of Ireland has reportedly been struck by the ransomware group **Alphv** (aka, BlackCat). The attack resulted in the University closing down while the incident was investigated, and is a reminder that schools and educational establishments are often considered fair-game by cyber criminals. **Alphv** have struck Universities on 3 previous occasions and schools on 2 occasions, suggesting that they have been opportunistically targeted, unlike **Vice Society** who have a victimology that heavily targets the education sector, with schools making up 36% of their targets in 2022.

2.4 The $10k ransomware manual

Cyber threat intelligence company Prodaft have acquired a document titled "Manual for work with networks 2.0", which is reportedly being sold online for $10k and is a guide on how to conduct and carry out ransomware attacks. Some topics included in the guide are:

- How to gather credentials from hashes
- How to identify and brute-force VPN servers
- How to identify critical servers and gain access
- How to takeover ESXi systems (ESXiArgs anyone?)

This sort of manual is commonplace on hacker forums and dark web markets, what is interesting is that it includes advice on whom to target but also whom to avoid, suggesting that another Colonial Pipeline incident should be avoided.

2.5 TV provider Dish experience ransomware attack

The satellite TV provider Dish has experienced a ransomware attack that has reportedly caused issues with their products, services and internal systems. There are reports that the attack was on the companies ESXi servers and backups, and an 8-K submission (legal form to inform investors of incidents) has confirmed that the attack involved ransomware. Dish are continuing to recover from the incident, and state they are investigating the extent of compromise and what data has been exfilrated. At the time of writing, a threat actor has not claimed responsible for the attack, but we once again are reminded of the importance of patch management.

2.6 Newcomers: Nevada

A new ransomware group called **Nevada** has emerged, with Resecurity gaining access to their affiliate dashboard and lockers, allowing insight into how the group and their malware works.

Nevada appear to be a standard RaaS operation who are able to target Windows and Linux/ESXi environments. The group do have a live dark web leak site, but at the time of writing there are no entries.

2.7 Newcomers: Mimic

Researchers at Trend Micro have released a technical report on a ransomware variant they have called **Mimic**, which has been active since June 2022. **Mimic** makes use of a novel technique, which involves the abuse of a legitimate API for a tool called **Everything**, which is a Windows filename search engine, using it to quickly locate files on a system that are to be encrypted. This is likely in an attempt to streamline and speed up the attack process, “time = money” is a universal equation apparently, even amongst criminals.

3 Other notable highlights in brief

3.1 GoAnywhere exploitation

Throughout February a vulnerability (CVE-2023-0669) in Fortra's product GoAnywhere has been widely exploited, leading to compromises and infection with ransomware.

GoAnywhere is a secure managed file transfer (MFT) tool, that is widely used in enterprise environments. The vulnerability is a cross-site request forgery, which exists due to the way GoAnywhere handles in-browser authentication. Unfortunately, threat actors have figured out that this can be exploited on GoAnywhere instances which are set up with the administration port (8000 or 8001) exposed to the internet. Proof-of-concept (PoC) code is freely available only and exploitation is trivial, which has resulted in threat actors targeting systems en masse.

The majority of these compromises have been conducted by the multi-point of extortion ransomware group **Clop**, a Russian cybercriminal group associated with **EvilCorp** the gang behind **TrickBot** and **Dridex**.

Fortra released updates for GoAnywhere which have resolved the issue, but are reliant on organizations having good patch management processes.

3.2 Zoho ManageEngine exploitation

A vulnerability in Zoho ManageEngine (CVE-2022-47966) has been heavily exploited this month, despite a patch being available since October 2022. The vulnerability exists due to the use of an outdated third party dependency called Apache Santuario, highlighting the problem of supply chain and relying upon dependencies, and results in RCE.

The vulnerability is being exploited by several threat actors, with different motivations, including, initial access brokers, ransomware groups and those interested in espionage. Internet analysis company Greynoise are tracking the campaigns, and 12 unique IP addresses are currently associated with the exploitation.

WithSecure™ Threat Intelligence has been tracking a campaign related to DPRK in which a number of ManageEngine services have been exploited, almost certainly on an opportunistic basis. These attacks could have been prevented if organizations had patch management plans that ensured updates occurred in a timely manner.

3.3 KeePass problems

The popular password management tool KeePass is under scrutiny at the moment, as there's a PoC available which allows a local attacker to make changes to the KeePass configuration file, inserting a trigger which exfiltrates clear-text versions of stored passwords to an attacker C2.

Security implications of this are clear, and while KeePass are aware of the issue, the following statement was posted on their 'Security Issues' bulletin board:

"*An attacker who has write access to the KeePass configuration file can modify it maliciously (for example, he could inject malicious triggers). This is not really a security vulnerability of KeePass though.*" - Arguing that if an attacker already has WRITE access access to a user profile directory then the attacker has enough control over a system to perform other malicious actions. While this is true, WithSecure™ believe in a strong defence in depth approach, and as attractive targets to threat actors, password vaults should be designed to be as resilient as possible even in the face of a system compromise.

3.4 QR code phishing

James Slaughter of Fortinet has published a report on a recent QR code phishing campaign that is targeting Chinese language users. Malicious QR codes are fairly rare, but Trend Micro note they can be used in various ways by threat actors. In the campaign discussed by Slaughter, targets received phishing emails containing office documents, and embedded within these documents was a QR code that would direct users to a credential harvesting page. This is an interesting approach, as it isn't relying upon macros or malicious code, but is instead using pretexting to influence users to interact with the QR code. This is just another example of how threat actors are finding new ways to phish bypass the increased protections against malicious readable hyperlinks and macros.

As always, one of the best lines of defense in phishing is the education of users, including the use of uncommon tactics like the use of QR codes.

3.5 Sh1mmer exploit can unenroll managed Chromebooks

Chromebooks are becoming popular in enterprise environments, thanks to their low cost and ease of management thanks to being part of the Google ecosystem. These Chromebooks are often managed, meaning that an IT admin is in charge of the device and changes require their authorization and access is somewhat limited for the intended user.

This is of course a security best practice, but there is now an exploit available called Sh1mmer, which can unenroll these devices, allowing the end user to make their own changes, and use the device without oversight. This might be attractive to people who want to use their work device for non-work means, (which we definitely don't recommend). Unmanaged devices used in enterprise environments create a much higher risk of compromise, as malware or vulnerable software could be installed by the user, and expose the wider enterprise network to infection/compromise.

3.6 IceBreaker target gaming/gambling companies

Website Security Joes have published a report on a campaign called **IceBreaker**, which is targeting the gaming and gambling sector. The attacks are quite unusual as they are specifically targeting the human operated customer chat/helpdesk functions on target websites. The threat actors are pretexting a supposed problem, and sending a malicious .lnk file via the chat function, disguised as a screenshot. The final payload is a remote access trojan (RAT), but the motivation behind these attacks is currently unknown.

Social engineering is becoming a popular technique and is now a part of many attacks, especially pretexting as it increases the likelihood of user interaction. It's vital that organizations provide appropriate training on the dangers of social engineering, and to be cautious when receiving files, even when part of what appears to be a legitimate exchange.

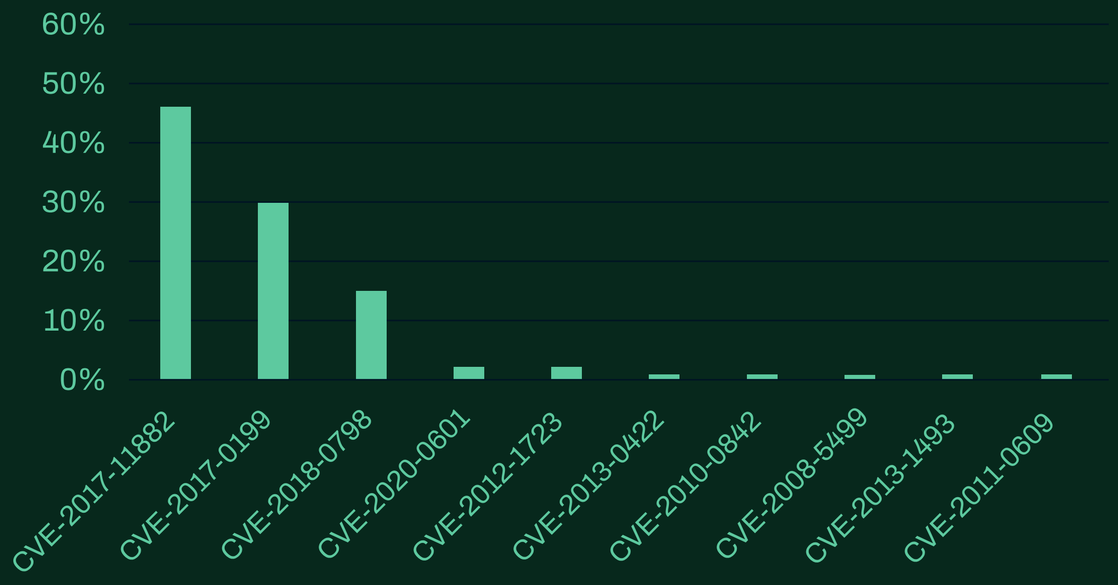
4 Threat data highlights

4.1 Exploits

The following data was captured throughout January 2023. There's little change across the vulnerability exploitation landscape again this month, with old favorites such as CVE-2017-1182, CVE-2017-0199 and CVE-2017-0147 all continuing to score highly, which are all vulnerabilities relating to Windows/Microsoft Office.

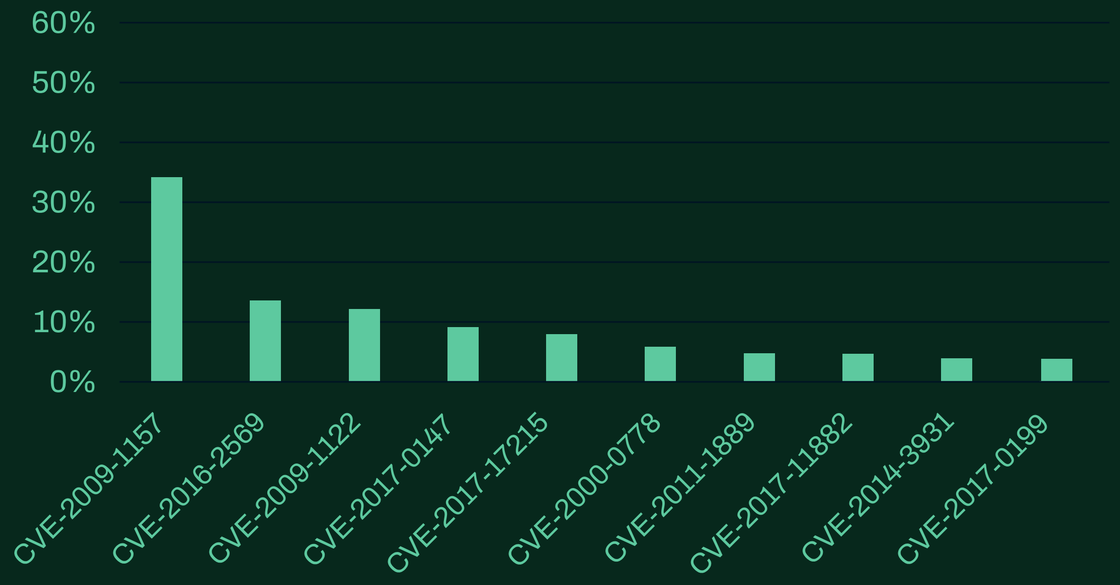
CVE-2020-0601 is a new entry, which is a spoofing vulnerability that exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates, meaning an attacker can make malicious files seem legitimate.

Top 10 exploits in the wild (WithSecure™ Telemetry)



WithSecure™ endpoint protection

Top 10 exploits in the wild (External Sources)



WithSecure™ endpoint protection

CISA’s known exploited vulnerabilities catalog

Since last month CISA have added 15 new exploited vulnerabilities to their catalog. 4 of which are rated as CRITICAL.

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2022-36537	ZK Framework AuUploader	High	"ZK Framework AuUploader servlets contain an unspecified vulnerability that could allow an attacker to retrieve the content of a file located in the web context. The ZK Framework is an open-source Java framework. This vulnerability can impact multiple products, including but not limited to ConnectWise R1Soft Server Backup Manager."
CVE-2022-47986	IBM Aspera Faspex	Critical	"IBM Aspera Faspex could allow a remote attacker to execute code on the system, caused by a YAML deserialization flaw."
CVE-2022-41223	Mitel MiVoice Connect	Medium	"The Director component in Mitel MiVoice Connect allows an authenticated attacker with internal network access to execute code within the context of the application."
CVE-2022-40765	Mitel MiVoice Connect	Medium	"The Mitel Edge Gateway component of MiVoice Connect allows an authenticated attacker with internal network access to execute commands within the context of the system."
CVE-2022-46169	Cacti	Critical	"Cacti contains a command injection vulnerability that allows an unauthenticated user to execute code."
CVE-2023-21715	Microsoft Office	Medium	"Microsoft Office Publisher contains a security feature bypass vulnerability which allows for a local, authenticated attack on a targeted system."
CVE-2023-23376	Microsoft Windows	High	"Microsoft Windows Common Log File System (CLFS) driver contains an unspecified vulnerability which allows for privilege escalation."
CVE-2023-23529	Apple	Under Review	"WebKit in Apple iOS, MacOS, Safari and iPadOS contains a type confusion vulnerability that may lead to code execution."
CVE-2023-21823	Microsoft Windows	High	"Microsoft Windows Graphic Component contains an unspecified vulnerability which allows for privilege escalation."
CVE-2015-2291	Intel Ethernet Diagnostics Driver	High	"Intel ethernet diagnostics driver for Windows IQVW32.sys and IQVW64.sys contain an unspecified vulnerability that allows for a denial-of-service."
CVE-2022-24990	TerraMaster OS	High	"TerraMaster OS contains a remote command execution vulnerability that allows an unauthenticated user to execute commands on the target endpoint."
CVE-2023-0669	Fortra GoAnywhere	High	"Fortra (formerly, HelpSystems) GoAnywhere MFT contains a pre-authentication remote code execution vulnerability in the License Response Servlet due to deserializing an attacker-controlled object."
CVE-2022-21587	Oracle	Critical	"Oracle E-Business Suite contains an unspecified vulnerability that allows an unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator."
CVE-2023-22952	SugarCRM	High	"Multiple SugarCRM products contain a remote code execution vulnerability in the EmailTemplates. Using a specially crafted request, custom PHP code can be injected through the EmailTemplates."
CVE-2017-11357	Telerik UI for ASP.NET AJAX	Critical	"Telerik UI for ASP.NET AJAX contains an insecure direct object reference vulnerability in RadAsyncUpload that can result in file uploads in a limited location and/or remote code execution."

5 Research highlights

5.1 Detecting OneNote Abuse

Riccardo Ancarani and Jojo O'Gorman of WithSecure™ have produced research on **Detecting OneNote Abuse**, the full report is available here.

As discussed in our Monthly Highlights section, a report was published last August by Emeric Nasi, which examined how OneNote could be abused by threat actors/penetration testers to deliver malware.

The research by WithSecure™ looks at the different ways OneNote can be abused, and has the following case studies, providing detection and prevent information on each:

- Embedding malicious executables within OneNote sections/ pages.
- Use of embedded content that is executed with living-off-the-land binaries (LOLBins), such as HTA, CHM, CPL, XLL and LNK files.
- Use of Right-to-Left-Override (RTLO) to spoof the extension of files embedded in OneNote sections.
- Despite OneNote being silently patched, malicious office documents could still be embedded and Mark-of-the-Web (MOTW) protections bypassed, through pretexting/social engineering.

The full report goes into different detection methods for OneNote abuse and makes the following conclusions:

- If possible, block direct download of one and onepkg files at the proxy level
- If possible, block .one and .onepkg mail attachments
- Monitor the operations of the OneNote.exe process, especially when a .one file is downloaded from the internet
- Pay particular attention to process creation events associated with common LOLBins
- File write operations should also be monitored closely

5.2 Analysis of YouTube USDT crypto scams

Andrew Patel of WithSecure™Intelligence has released analysis on an ongoing campaign of YouTube USDT crypto scams, the full report is available here.

WithSecure™ Intelligence has discovered thousands of videos advertising fraudulent web-based apps that pose as USDT (Tether) investment schemes. These videos, hosted on YouTube, promise returns that scale on the amount of currency invested. YouTube channels with significant numbers of subscribers and view counts post new videos of this type on a daily basis. Some of the participating channels are even YouTube verified accounts.

The full report details the anatomy of the videos and apps behind this scam, analyses two associated scam apps in detail, explores the #usdtmining YouTube hashtag, describes blockchain analysis methodology used on crypto wallets associated with the scam, and finally presents recommendations for YouTube and some final conclusions.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure