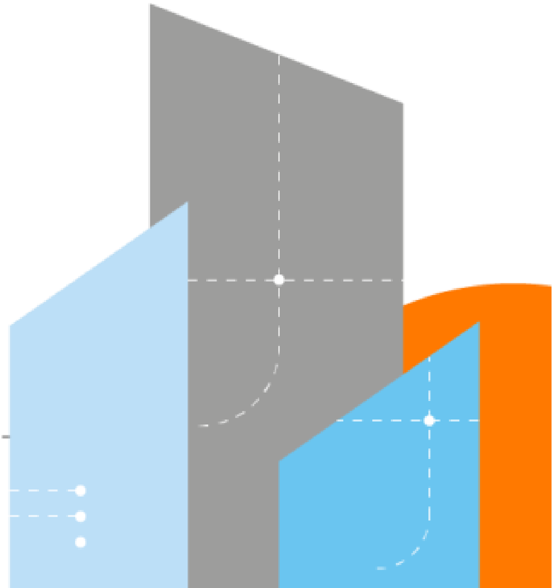
Orange
Cyberdefense

Security Intelligence

Monthly Report

February 2022



Unrestricted

CONTENTS

INTRODUCTION

The situation in Ukraine has taken a turn for the worst with the Russian military invading the country. This action was prefaced with cyberattacks including Distributed Denial of Service, defacements, and attacks involving malware masquerading as ransomware where in fact it turned out to be 'wiperware'.

Some in the cyber community have chosen sides. Hacktivists going under the Anonymous banner have claimed responsibility for attacks launched against Russian government and state-owned media entities. On the opposite end of the spectrum, the Conti Cyber Extortion group suffered their own data leak. The leak was apparently facilitated by a Ukrainian Conti member in retaliation to Conti leadership pledging allegiance to Russia. Chat logs, cryptocurrency accounts, and other sensitive details of the Conti group were leaked.

Thus far cyberattacks associated with the war seem to have been isolated to Ukrainian, Russian, and Belarusian controlled networks. Be prepared as this could change at a moment's notice.

Orange Cyberdefense is actively following the evolution of the current conflict between Russia and Ukraine. Please see https://orangecyberdefense.com/global/blog/threat/ukraine-russia-cyber-conflict-observations-what-you-should-do-what-we-are-doing/ for more information on this evolving situation.

At a glance

Thus far cyberattacks seem to have been isolated to the Ukrainian, Russian, and Belarusian controlled networks. Be prepared as this could change at a moment's notice.

Over the past year we reported on several zero-day vulnerabilities. This month is no exception with major vendors such as Google and Microsoft once again in the firing line. Google's Chrome browser has a significant market share and zero-day exploits against it can result in significant compromise. Google fixed 17 zero-day vulnerabilities in the Chrome browser. Other products that received fixes for zero-day vulnerabilities include Adobe's Magento eCommerce platform and the Zimbra email platform.

Open-source software is an important part of many software stacks. We were reminded of this in December 2021 with the Log4J vulnerability. This month we covered two vulnerabilities affecting open-source software. These vulnerabilities could result in remote code execution. The Samba project fixed a flaw in its Apple Netatalk module. The second flaw was present in the database project called Apache Cassandra. This flaw is due to a very specific non-standard configuring.

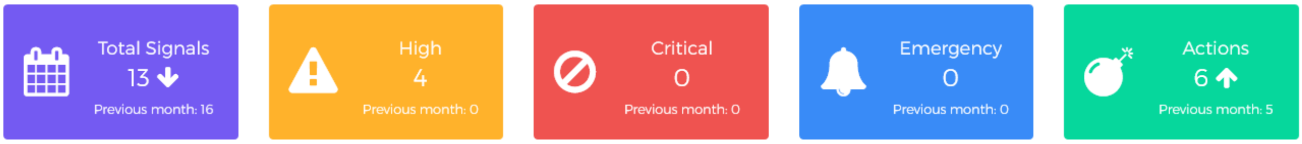
Phishing and Social Engineering attacks will remain effective as long as humans can still be tricked into performing tasks on behalf of attackers. In recent months attackers leveraged features of Microsoft's Office365 cloud applications to target executives of businesses. The cloud apps, if permitted by the victims, can allow an attacker access to sensitive information such as email and documents of the victim. This attack is possible due to excessive permission on a victims account that allow the user to grant permissions to the cloud app.

Cyber criminals have specialised in creating pieces of software for specific tasks such as wrapping malware in a bundle that is deployed when a victim opens a malicious attachment or is tricked into clicking a link through social engineering means. PrivateLoader is such a piece of malware that can be obtained through a 'pay-per-install' scheme. This new malware has been attributed for installing several other known malware strains.

Finally, Vodafone Portugal suffered a breach that impacted several of its services. The mobile network operator scrambled to restore its 4G/5G, text messaging, and television broadcasting services as a result of the cyberattack. Vodafone claims that no customer data has been breached.

OVERVIEW

In this section of the report we share some notable statistics and trends regarding our World Watch Advisory service, the issues we are discussing and the actions we are taking on your behalf.



Total Signals
13 ↓
Previous month: 16

High
4
Previous month: 0

Critical
0
Previous month: 0

Emergency
0
Previous month: 0

Actions
6 ↑
Previous month: 5

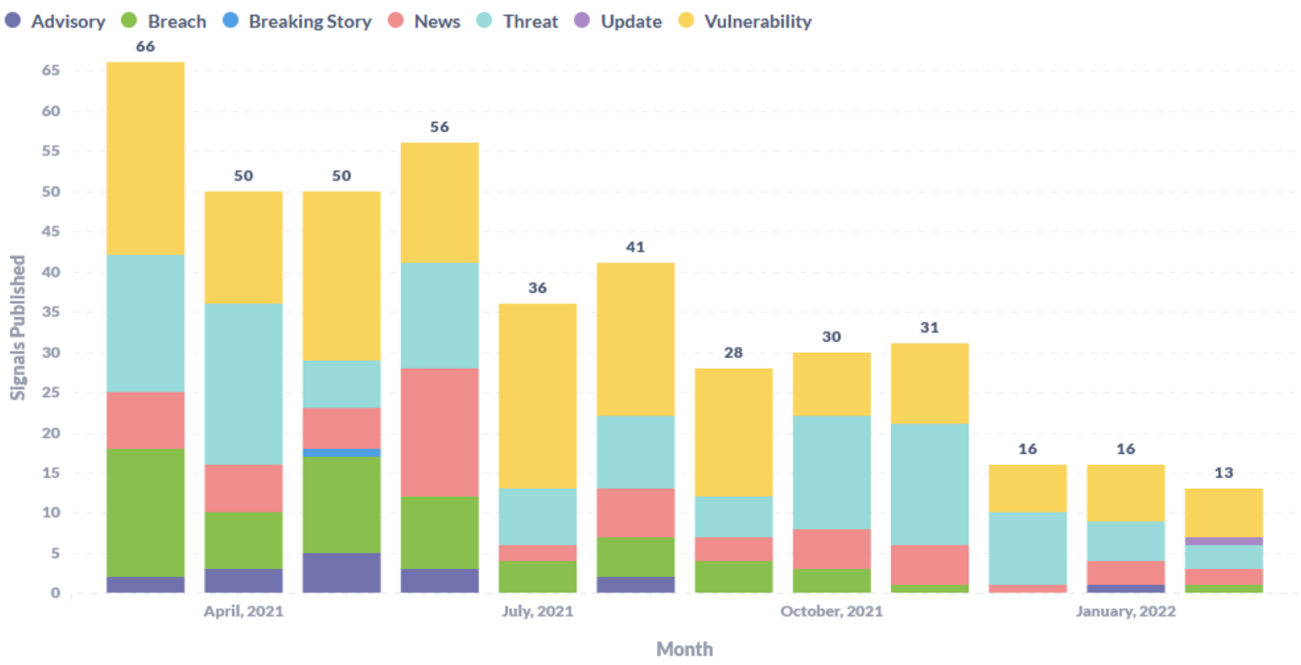
Signals Summary for February 2022

As stated previously, the number of total Signals published has been in decline for the past few months. This is not an indication that the number of threats or incidents have decreased but has been brought on by a change in the Signals service itself. Work is still ongoing to transition the Signals service which will then be rebranded as World Watch. This will involve a couple of changes of which one is the team responsible for generating the content, as well as the medium of communication.

Our 'Signals' are organised into seven distinct categories to help you understand what kind of message we are communicating. In the graph above you can track the number of unique Signals we have published, grouped by the seven categories:

- Advisory: A general security update worth noting and taking action on
- Threat: An actor, campaign, or attack technique in the wild that is significant
- News: General news from the security space. Probably not requiring any action.
- Breaking Story: A significant security development or event that is not yet fully understood, but important enough to take note of.
- Breach: News about a publicly-reported compromise that resulted in confidential data being leaked or stolen.
- Emergency: An urgent Advisory about a significant new threat or vulnerability that almost certainly requires immediate action. Emergency advisories are automatically sent to all customers and correspond with the activation of our own internal 'Major Incident' process.
- Update: A further development, clarification, escalation or correction to an advisory we have previously published under one of the categories above.

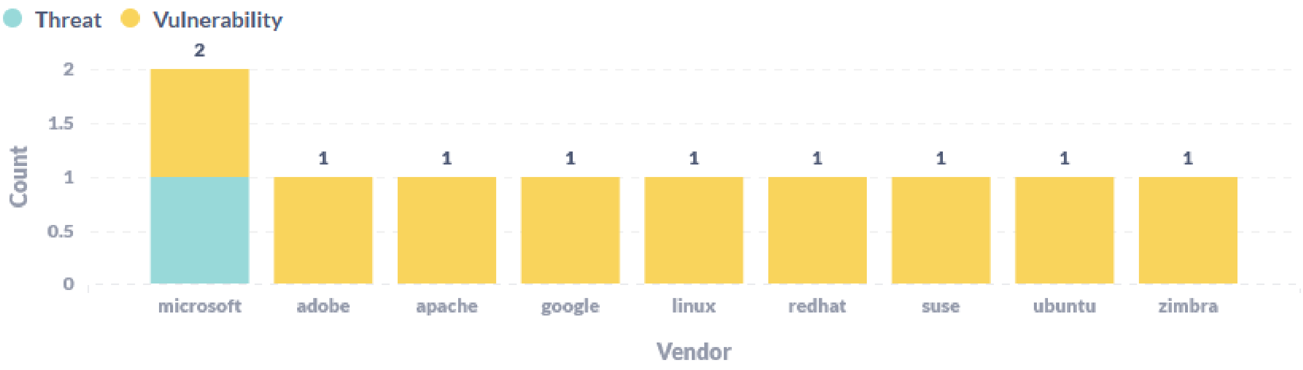
Categories – Monthly Breakdown



The distribution of Signals across 2021 is tapering downward. The past three months showed a significant drop in Signal volume. The low volume of Signals does not necessarily translate into the reduction of overall threats. There are still an increasing number of threats present in the cyber landscape and businesses need to proactively work to reduce the number of vulnerabilities in their estate.

Please note: This section of the monthly reports will be changed in future versions due to changes in how the underlying 'World Watch' service is being delivered.

Technologies Affected



The chart above summarises the technology vendors that were referenced in our Signals across the various categories this month.

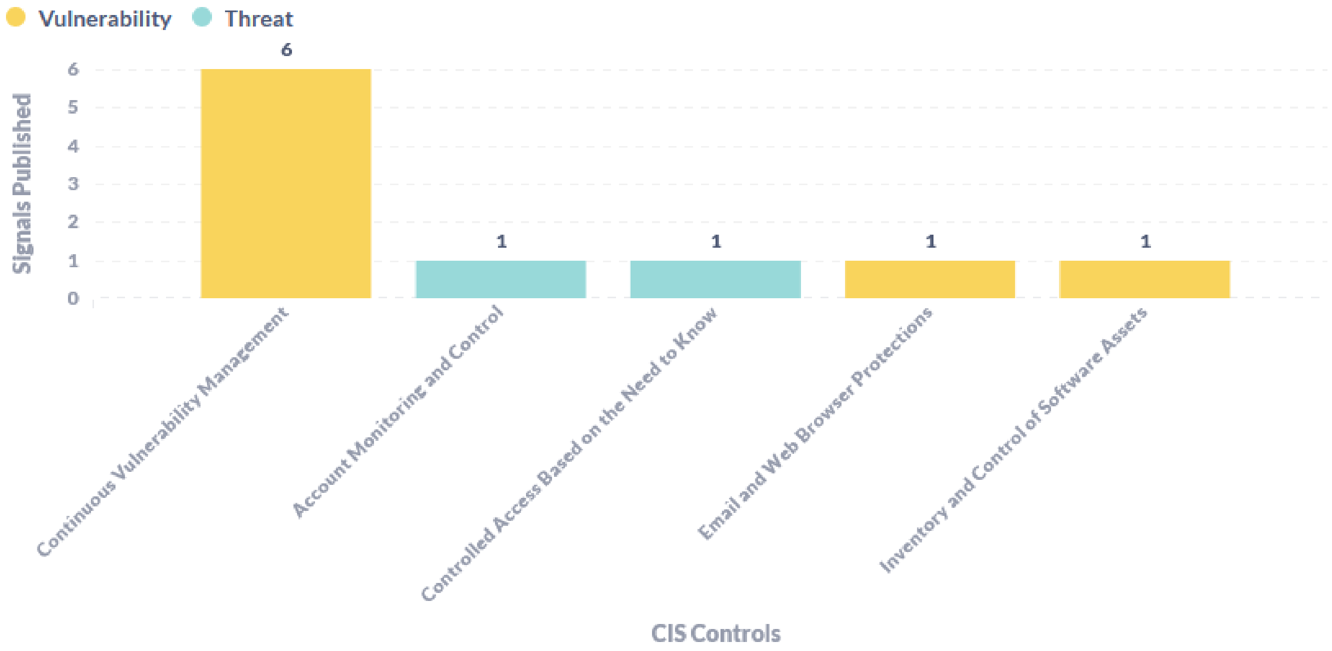
The inclusion of Linux, RedHat, Suse, and Ubuntu relates to a remote code execution vulnerability in Samba, tracked as CVE-2021-44142. This vulnerability is a protocol level flaw in the compatibility module used by Samba to interface with Apple Netatalk 3 services.

Microsoft is represented consistently due to its monthly security updates released on every second Tuesday of each month. February saw a lower than usual number of vulnerabilities being fixed by Microsoft, which could help teams to catch up with their patch rollouts.

Please note: This section of the monthly reports will be deprecated in future versions due to changes in how the underlying ‘World Watch’ service is being delivered.

Our Recommendations

Whenever we include a recommendation in a Signal, that recommendation is mapped to the CIS Top-20 controls framework (see https://www.cisecurity.org/controls/cis-controls-list/). This allows us to present a view on which standard security controls are occurring most frequently in our advisories



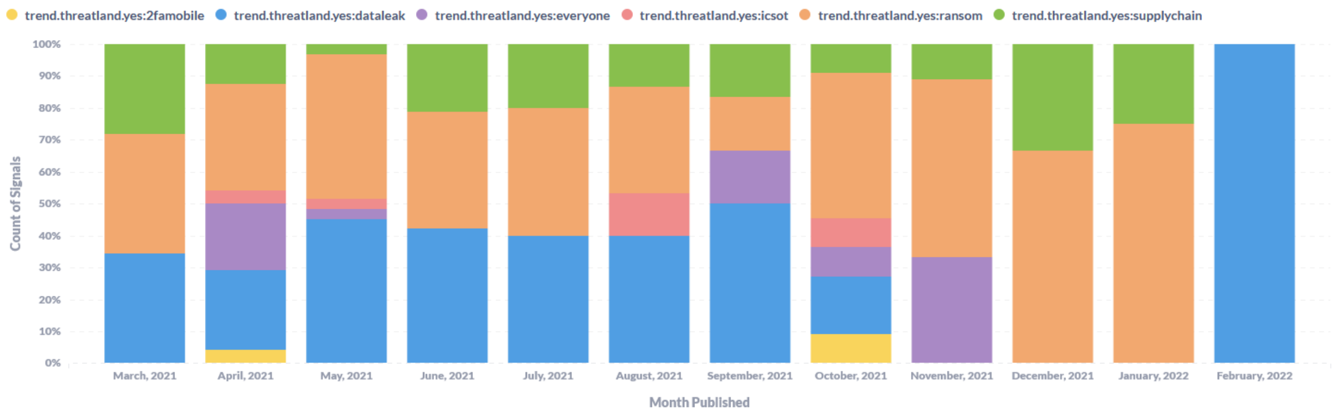
This chart summarises the recommendations our analysts have made in our Signals, separated between Threats and Vulnerabilities on the one hand, and the control failures we recognised in breaches, on the other.

This month sees the inclusion of ‘Account Monitoring and Control’, ‘Controlled Access Based on Need to Know’, and ‘Email and Web Browser Protections’. The first two CIS controls are directly linked to the ‘least privilege’ principal. Limiting access to resources and limiting what actions can be performed on these resources are becoming more and more important in the fight against ransomware. Similarly, monitoring actions and identifying violations of policies is an important tool in enforcing segmentation of roles and privileges. These controls are important in the bigger scheme of things, especially the looming threat of phishing. Attackers can use this technique to steal credentials and then use that to gain access to services exposed on the Internet or leverage excessive privileges to gain a strong foothold on infrastructure. Businesses need to ensure their budget for dealing with phishing is adequate to deal with the evolving phishing threat.

Please note: This section of the monthly reports will be deprecated in future versions due to changes in how the underlying ‘World Watch’ service is being delivered.

General Trends

All the Signals we publish are also tagged with markers for significant global security trends we track in our efforts to better understand the security landscape.



Data leak or data breaches finally featured this month after a long absence. This lone data breach impacted Vodafone Portugal.

February 2022 was the first time in more than a year that we published Signals that did not carry the ransomware theme. The reality is that several news stories did cover ransomware, we simply chose to cover other topics. By now ransomware news is par for the course, with the main variable being the victims. Supply Chain news is also a regular news topic, but stories with significant impact failed to make the cut for February 2022.

Please note: This section of the monthly reports will be changed in future versions due to changes in how the underlying ‘World Watch’ service is being delivered.

Editor's Notes (Beta)

This section is relatively new and was introduced in the January 2022 monthly report. Here the team will provide commentary on a news item, expansion on something specific such as a single incident, or could be as expansive as coverage on trends observed in the threat landscape.

Diana

Cryptocurrency – fighting crime or chasing the wrong numbers?

Last year, the US National Cryptocurrency Enforcement Team (NCET) was established for the purpose to assist tackling criminal misuse of cryptocurrencies and digital assets. In mid-February 2022, Eun Young Choi, NCET's first director was appointed by the U.S. Department of Justice (DOJ). Amongst other tasks, NCET will assist in tracing and recovering assets that were stolen through cyber extortion operations such as ransomware and fraud. Similar efforts were announced by the Federal Bureau of Investigation (FBI) intending to launch their own unit to track and seize illicit cryptocurrency payments. These developments do not come as a surprise, given that the overall perception is that illicit activities using cryptocurrency are rising dramatically.

However, I say *perception* because it is always important to put this into perspective. Cryptocurrency has until now defended its reputation to be hard to trace, the establishment of a government unit trying to do exactly that can seem invasive for some, even if it is established with the goal of fighting crime.

Indeed, the Chainalysis 2022 Crypto Crime Report points out that the value of illicit transactions has reached an all-time high ($14 billion in 2021, $7.8 billion in 2020). However (and this is important) if we put this into perspective, the overall use of cryptocurrency has grown so fast that the actual share of criminal transactions is **at an all-time low**.

This data is of course limited to Chainalysis' tracking capabilities. The illicit transactions they have been tracking grew to $15.8 trillion in 2021, an increase of 567% to the previous year of which only 0.15% (0.62% in 2020) involved illicit addresses.

It will therefore be interesting to observe how successful government involvement in this fight against cybercrime will be, but also how invasive to the technology itself.

Carl

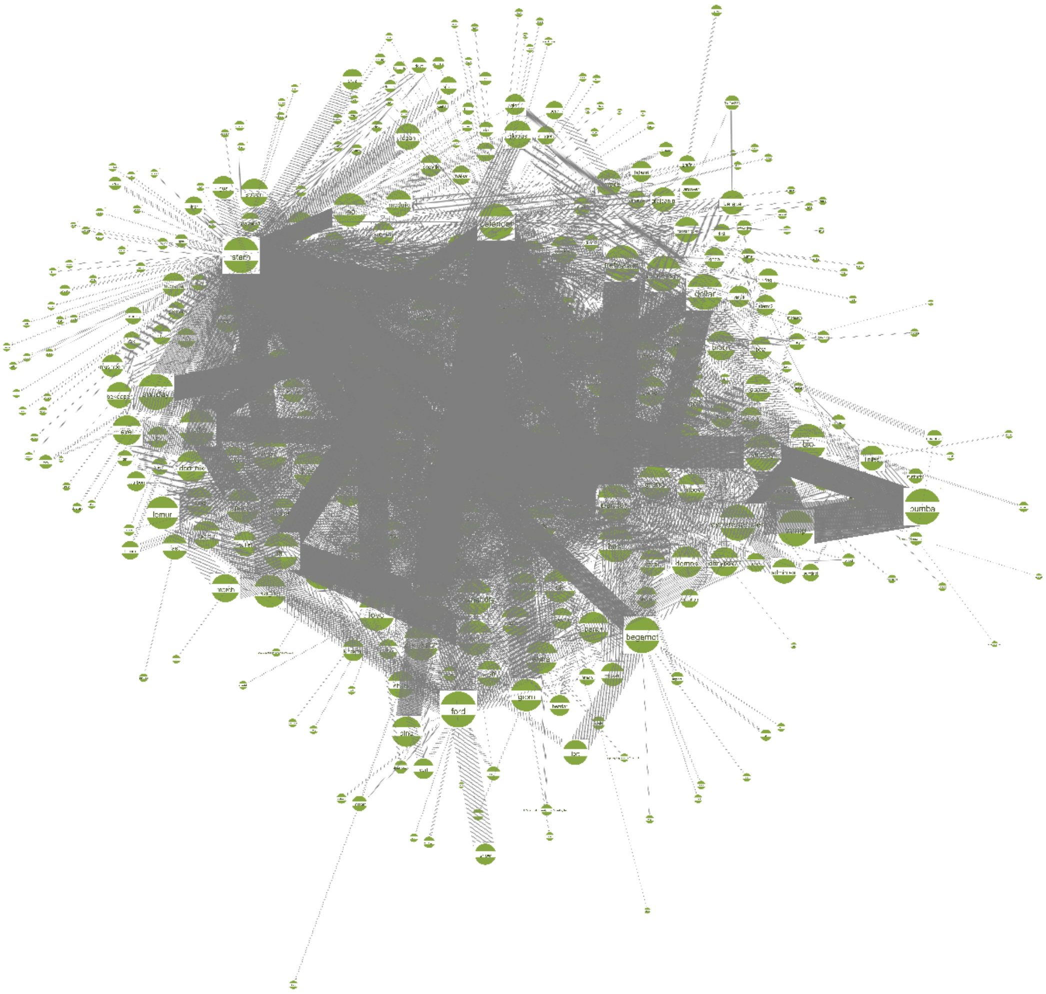
Unexpected Consequences

As also touched on below, the war against Ukraine has had some unexpected consequences. The most notable was the announcement from the Conti cyber-extortion group of their support for Russia with a threat to strike back at enemies who carried out cyberattacks or other war activities against Russia.

The group did quickly backpedal somewhat though and softened their message by taking a more neutral stance. Stating that they didn't ally themselves with any particular government, they reiterated however they would target “Western warmongers” in revenge of any attempts to target Russian critical infrastructure. The revised announcement came too late and did nothing to mollify what is believed to be either a disgruntled Ukrainian member of the group or a Ukrainian security researcher. In response to the group pronouncement, this individual proceeded to leak internal data from the group containing details of attack infrastructure, bitcoin addresses, source code, and organisational structure, as well as internal chat logs.

As soon as these leaks started appearing via the “Conti leaks” Twitter account, security teams were scrambling to digest and analyse the data contained within, and Orange Cyberdefense was no exception. Whilst we were already monitoring Conti since July 2020, this was limited to information published on their leak site and some of their negotiation discussions. These leaks now provide much more concrete details of their organisation which in theory can be used to detect and protect against attacks and will require the group to move their operations to new infrastructure. A coordinated working group within Orange Cyberdefense is currently analysing the vast amount of data that was leaked. All the resultant Cyber Threat Intelligence has been captured to our intelligence ‘Datalake’ and further detailed findings will be published when appropriate.

An initial high-level analysis was published on our blog and can be found here: https://orangecyberdefense.com/be/blog/cyberdefense/analysis-of-the-leaked-internal-conti-chat/.



Charl

On Kaspersky and Balkanization

The war by Russia against Ukraine has had several bizarre side effects. The internal rift within the 'Conti' Cyber Extortion group came has a huge surprise to many of us, for example. The emerging risk and security questions surrounding Anti-virus and Endpoint Security vendor Kaspersky – come as less of a surprise.

The concerns surrounding Kaspersky are nicely summarized here - https://cybernews.com/security/kaspersky-neutral-stance-in-doubt-as-it-shields-kremlin/ -

"Kaspersky, being a well-recognized brand worldwide, has always been haunted by its origins and put efforts to shake ties to the Russian government, including moving its core infrastructure from Russia to Switzerland and unsuccessfully suing the US government for its decision to ban the use of Kaspersky Lab within the US government.

The company emphasizes that it does not share any user data with law enforcement. However, a closer look at Kaspersky's activities exposes its close business ties with key players in Putin's Russia".

Businesses worldwide are scrambling to assess and respond to the apparently increased risk associated with using Kaspersky considering the war against Ukraine.

This is not a new development, however. Nor an isolated one. The Kaspersky story started as far back as 2015.

Come September 2017, the Department of Homeland Security (DHS) instructed federal civilian agencies to remove Kaspersky software on the grounds that the Russian government "could capitalize on access provided by Kaspersky," in a manner which "directly implicates U.S. national security" (https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html).

Senator Marco Rubio noted the widespread use of Kaspersky Anti-Virus within the US government during a congressional hearing. He asked, "Would any of you be comfortable with the Kaspersky Lab software on your computers?"

"A resounding no from me," said Director of National Intelligence Daniel Coats (https://www.washingtonpost.com/investigations/local-governments-keep-using-this-software--but-it-might-be-a-back-door-for-russia/2017/07/23/39692918-6c99-11e7-8961-ec5f3e1e2a5c_story.html).

The subsequent decision to ban the Kaspersky anti-virus software from all US government computers follows a months-long international inquisition over whether the cybersecurity giant's products could really be trusted.

A U.S. IT retail giant followed suit by removing the firm's products from their shelves.

The move by the DHS apparently followed an allegation by Israel about Kaspersky's' collection, deliberate or accidental, of US cyber tools from a contract worker's personal computer. Kaspersky explained that an unnamed NSA contractor had the Kaspersky security software installed on his home computer. When, at some point, he downloaded and tried to run a pirate license key generator for the Microsoft Office suite, Kaspersky blocked it because the keygen was infected with a known back door. The intrepid American spook then did the only logical thing, and disabled Kaspersky's anti-virus so that his crack program could run, before activating it again. At this point Kaspersky detected and blocked the backdoor in the keygen, but also spotted a trove of NSA hacking tools on his machine because of markers already familiar to Kaspersky from a 2016 NSA data leak.

This NSA consultant had selected the option to upload suspicious files to Kaspersky for further analysis.

We may never know if this Kaspersky story is true. But it doesn't really matter whether their collection of classified US cyber tools was deliberate or accidental, or whether the Russian government had any influence over their actions.

At its root, this isn't about Kaspersky or even Russia. It's about an inherent tension between an Internet that is global as much as it is local and civilian as much as it is government and a geopolitical reality where those domains are still viewed as strongly separate.

Intelligence gathering, electronic warfare and psyops are nothing new, but the power of 'cyber' operations as a means of executing them has rapidly grown in the last decade. The world started to recognize its power when the Stuxnet attack against Iranian Uranium plants was revealed in 2010.

Cyber has since been rapidly adopted by security services as a powerful adjunct to traditional intelligence gathering and asymmetric warfare. Nation-on-Nation cyber-attacks are a daily occurrence. Their effects are increasingly being felt in the civilian domain, as was graphically demonstrated by the WannaCry and NotPetya attacks. Governments are in continuous low-velocity conflict with each other, and the Internet is a full-scale domain of war.

Cyberspace is also densely occupied by civilians. The people who build it, the technologies they build and the people they sell it to are mostly civilian too. This has the inevitable effect of dragging the civilian world into the domain of international conflict. Now the military and civilian domains of the Internet are set on a collision course because every technology and every technology user are both of the Internet, and of a specific geopolitical entity.

Every cyber technology now has the potential to be a weapon or a target. Slowly but surely those technologies and the people who make them will be drawn into the fray, one side or another.

It's in this light that we should view the recent concerns about Kaspersky's political allegiances, and the consequence is a process called 'Cyber Balkanization'.

Cyber Balkanisation, first used in 2011, describes the Internet as splintering and dividing under the weight of technology, commerce, politics, nationalism, religion, and other interests. Some argue that this process is already taking place as countries seek to implement various forms of Internet censorship and control or enforce data protection, security, or privacy legislation.

The Kaspersky concerns, reasonable as they may be, now make it look like a tragic inevitability: As the west starts rejecting Russian and Chinese technologies, why wouldn't those two countries do the same? Pro-western allies like Israel would inevitably be painted with the same brush.

All the way up and down the computing stack governments and companies will be forced to choose vendors which they can politically trust. Smaller countries will be compelled to choose between one camp or the other as they can't possibly field their own computing stacks, and so the world gradually breaks apart until cyberspace is fully Balkanised.

China is already in the firing line and governments will increasingly see its technologies and systems being shunned. The degree of trust accorded to anti-virus software and the deep distrust with which Russia is viewed in the west serves to highlight what is really a fundamental problem for all governments; that software is developed all over the world and runs on sensitive computers without much thought to its origins or political affiliation.

That's all busy changing and we can safely assume that it won't just be western governments that think this way. Security giant Trend Micro is an American-Japanese multinational with global headquarters in Tokyo. Checkpoint is Israeli. Sophos is British and a great many more are American. Any government or corporation acquiring security software to run on sensitive computers would have to give some consideration to its country of origin and the potential influence that government might have over its development and operation. Why should Trend, Check Point, Sophos or McAfee be any less vulnerable to meddling by their own governments' security services than Kaspersky?

To me that's a tragedy. The Internet is a global phenomenon that promised to bind cultures and countries across the world, connecting us to a diversity of people with their thoughts, views, and unique orientations. If balkanization does continue to spread as I fear, that may well herald the final nail in the coffin for the vision that was once a free, open, and global network for all people.

Wicus

Identity and the (HTTP) Cookie

Multi-Factor Authentication (MFA) is one of the recommendations given to help protect user accounts against successful phishing attacks. The attacker can have the username and password, but without the additional factor, they will not be able to proceed with the authentication attempt. Only when all MFA tokens are supplied can a user's identity be verified. This identity is carried as a pseudo value also referred to as an HTTP cookie. Most of the web relies on the confidentiality of the identity carrying HTTP cookie. For each interaction with a designated web site the web browser must supply this identity-carrying token.

Phishing and social engineering attacks combined with a Person-in-the-Middle attack are arguably the biggest threat against Multi-Factor Authentication for the simple fact that the attacker can acquire a copy of the HTTP cookie used to actually identify the bearer.

The HTTP cookie concept was introduced by Lou Montulli while working at Netscape in 1994. Several technical advancements have been made over the years to protect against attackers abusing weakness in how cookies are accessed, and the web browser is ultimately responsible for implementing these protections to ensure attackers can gain access to sensitive cookies.

Why are HTTP cookies such a big deal? HTTP cookies are used to store information that can be tied to a web session, which in turn is associated with a user, or contain information that is used as part of the Single Sign-On (SSO) process to authenticate a user. If an attacker can get a copy of a cookie, then the attacker can gain access to the same account as the legitimate user, simply by copying the value and submitting it to a web site associated with the victim.

In the past attackers leveraged flaws in websites to steal cookies by using Cross-Site Scripting (XSS) flaws or benefitting from Cross-Origin Resource Sharing (CORS) misconfigurations. The introduction of special attributes on Cookies such as HttpOnly makes it theoretically impossible for attackers to use JavaScript to access and steal the cookie content.

Another way for an attacker to gain access to this 'HttpOnly' cookie is to intercept the HTTP traffic but is made difficult because of the confidentiality and integrity introduced by TLS. HTTPS by design does not allow anyone besides the service that provided proof of its identity through its digital certificate to access the content of the HTTP request. Technical attacks against SSL have been demonstrated in the past by researchers like Moxie Marlinspike with his SSLStrip tool, but once again browsers stepped up and built protections in to alert the user of such attempts. Thus, where HTTP Strict Transport Security (HSTS) is implemented, the browser will halt such attacks and refuse to proceed.

Another potent attack vector includes malicious browser extensions or addons. These third-party browser extensions have additional access to HTTP message streams and could be described as a Person-in-the-Browser attack. These extensions are in a very strong position to gain access to sensitive authentication material and more.

Detection of compromised accounts will therefore become an increasingly important control. The accuracy and sophistication of these detection and alerting controls will help in stopping compromise as early as possible. Simple behavioral traits such as geolocation of the IP impersonating the victim, as well as browser and device attestation will become important aspects to detect subterfuge.

Good News Cyber

A NetWalker ransomware gang affiliate operating out of Canada pleaded guilty to charges laid against him and was sentenced to 7 years in prison. The conviction involved five charges related to 'theft of computer data, payment of cryptocurrency ransoms, and participating in the activities of a criminal organization.' The NetWalker affiliate was complicit in at least 17 ransomware attacks totaling approximately $2.8 million dollars in damages. Law enforcement confiscated 720 Bitcoins and said the affiliate made approximately $27.6 million from ransomware activities.

The war on Ukraine will be devastating for the country. Just before the attack on the country the Ukrainian law enforcement authorities shared another successful arrest of people suspected of being part of a major phishing operation. The phishing operators targeted payment card details through spoofed websites. Five individuals were mentioned in the press release that managed to embezzle approximately 5 million hryvnias ($172,600). The attackers ran and operated their own web server infrastructure and created more than 40 phishing web sites. The Ukrainian law enforcement authorities have made a lot of progress in recent months, arresting several suspected cyber criminals.

DATA BREACHES

The attack on Vodafone Portugal was substantial. It affected nearly all aspects of the business, impacting its ability to deliver consistent 4G/5G services. The impact extended to text messaging and television broadcasting services.

Vodafone Portugal 4G and 5G services down after cyberattack

Date: 09 February 2022

Vodafone Portugal suffered a cyberattack causing country-wide service outages, including the disruption of 4G/5G data networks, SMS texts, and television services.

MALWARE AND EXPLOITS

Ukraine has been at the receiving end of Russian aggression for a long time. Cyberattacks against Ukraine have escalated ever since the Russian annexation of Crimea in 2014. February 2022 saw a repeat of cyberattacks against government and financial institutions in Ukraine. This proved to be a precursor to Russia launching a full-scale invasion of Ukraine. The cyberconflict has started to spill beyond Ukraine as some hacktivists started to show their support by targeting Russian government and statement entities.

Phishing and Social Engineering attacks are difficult to fight due to its high rate of evolution. Attackers have successfully abused features of trusted cloud services providers such as Microsoft's Office 365. This allowed the attackers to obtain access to the phished accounts with follow on actions.

A malware-as-a-service tool called PrivateLoader has seen increased popularity. This malware is typically used by attackers as part of early-stage attacks against their victims. This type of tool is not new and the most infamous has been Emotet in recent years, before its partial takedown by law enforcement in 2021.

CEO Office365 accounts targeted by OiVaVoii hacking campaign through compromised OAuth apps

Date: 03 February 2022

Threat analysts have observed a new campaign named 'OiVaVoii', targeting company executives and general managers with malicious OAuth apps and custom phishing lures sent from hijacked Office 365 accounts.

Pay to play PrivateLoader spreads Smokeloader, Redline, Vidar malware

Date: 10 February 2022

The pay-per-install malware is one of the most popular loaders on the market today.

Microsoft says 'destructive malware' being used against Ukrainian organizations

Date: 28 February 2022

Security teams at Microsoft said the malware first appeared on victim systems in Ukraine on January 13.

VULNERABILITY MANAGEMENT

February 2022 saw several vulnerabilities that have been exploited by attackers before fixes were available. Once again Google Chrome browser had to receive fixes for a zero-day exploit.

Other zero-day vulnerabilities were reported and fixed in Microsoft Windows operating system, Adobe's Magento eCommerce solution, and Zimbra email platform.

The Samba open-source project released details of a remote code execution vulnerability that could be exploited when an attacker targets the Apple Netatalk module. Several Linux based distributions issued fixes for this flaw.

The open-source database project Cassandra, that is under the auspices of Apache Software Foundation, received a fix for a remote code execution vulnerability. Fortunately, this is for a very specific configuration set.

Samba 'Fruit' Bug Allows RCE, Full Root User Access

Date: 02 February 2022

The issue in the file-sharing and interop platform also affects Red Hat, SUSE Linux and Ubuntu packages.

Operation EmailThief: Zero-day XSS vulnerability in Zimbra email platform revealed

Date: 04 February 2022

A zero-day bug in the Zimbra email platform is reportedly under attack.

Microsoft February 2022 Patch Tuesday fixes 48 flaws, 1 zero-day

Date: 09 February 2022

Today is Microsoft's February 2022 Patch Tuesday, and with it comes fixes for one zero-day vulnerability and a total of 48 flaws.

Adobe: Zero-Day Magento 2 RCE Bug Under Active Attack

Date: 15 February 2022

The vendor issued an emergency fix on Sunday, and eCommerce websites should update ASAP to avoid Magecart card-skimming attacks and other problems.

Google Chrome emergency update fixes zero-day exploited in attacks

Date: 15 February 2022

Google has released Chrome 98.0.4758.102 for Windows, Mac, and Linux, to fix a high-severity zero-day vulnerability used by threat actors in attacks.

High-Severity RCE Bug Found in Popular Apache Cassandra Database

Date: 17 February 2022

On the plus side, only instances with non-standard not recommended configurations are vulnerable. On the downside, those configurations aren't easy to track down, and it's easy as pie to exploit.

NOTEWORTHY

Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps

Date: 11 January 2022

Users of popular open-source libraries 'colors' and 'faker' were left stunned after they saw their applications, using these libraries, printing gibberish data and breaking. Some surmised if the NPM libraries had been compromised, but it turns out there's more to the story.

Microsoft disables Excel 4.0 macros by default to block malware. Google Drive now warns you of suspicious phishing, malware docs.

Date: 26 January 2022

Microsoft has announced that Excel 4.0 (XLM) macros will now be disabled by default to protect customers from malicious documents. Google is rolling out new warning banners in Google Drive to alert users of potentially suspicious files.

Russia charges 8 suspected REvil ransomware gang members

Date: 17 January 2022

Eight members of the REvil ransomware operation that have been detained by Russian officers are currently facing criminal charges for their illegal activity.

DOJ seizes $3.6 billion in crypto from 2016 Bitfinex hack, arrests New York couple

Date: 10 February 2022

Ilya Lichtenstein and his wife Heather Morgan are accused of laundering the proceeds of 119,754 bitcoin that were stolen from Bitfinex's platform in 2016.

US says Russian state hackers breached cleared defense contractors

Date: 18 February 2022

Russian-backed hackers have been targeting and compromising U.S. cleared defense contractors (CDCs) since at least January 2020 to gain access to and steal sensitive info that gives insight into U.S. defense and intelligence programs and capabilities.