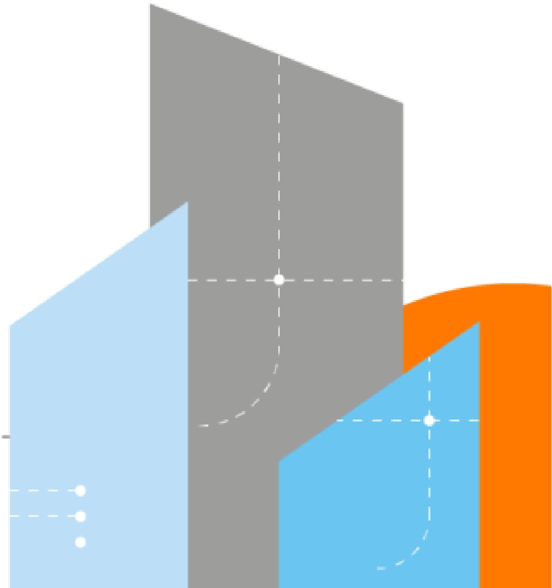
Orange
Cyberdefense

Security Intelligence

Monthly Report

January 2022



Unrestricted

CONTENTS

INTRODUCTION

Cyber Extortion and Ransomware have consistently featured in our Signals for more than a year. This threat is evolving and adapting to actions taken by businesses, law enforcement, and geopolitical tensions. It’s almost like a hydra. Cut-off one head and two spawn in its place. This month we reported on two new ransomware groups called Night Sky and White Rabbit.

The tension between Ukraine and Russia is increasing with Russia flexing its military might. Cyberattacks were launched against Ukrainian government sites that involved defacements, but also malware called WhisperGate that masqueraded as ransomware, but instead only destroys data with no hope of recovery. Information on this attack is coming in slowly so it’s still premature to attribute these attacks to Russia.

Log4Shell was considered a major cybersecurity event due to what many believed to be an extremely dangerous vulnerability. To date we have not yet observed mass exploitation of this flaw, however, with follow on actions like we saw with WannaCry or NotPetya in 2017. Log4Shell is well suited for targeted attacks but does not scale the same as protocol level attacks. At the same time, the call to arms of the cyber security community mobilised large numbers of system administrators and business leaders. This action possibly led to many businesses eliminating low hanging fruit making it very difficult for attackers to capitalise on the flaw.

Mass exploitation using self-replicating or wormable malware requires a vulnerability to be exposed in a manner that is easy to reach. This risk is arguably more real for a recent fix (CVE-2022-21907) that Microsoft released for the HTTP driver present on the latest desktop and server versions of the Windows operating systems. Web servers are typically accessible over the Internet, meaning that unpatched HTTP IIS web servers could possibly be exploited and turned into a malware spreading device. Added to this, the attacker can take control of this compromised device to launch other attacks such as Distributed Denial of Service attacks, send spam, or pivot off that compromised host into the internal network. The latter would be valued by cyber extortion or ransomware groups as this could mean easy access to steal data and launch their malware to encrypt the internal networks.

A decade old vulnerability in Polkit, found in popular Linux distributions, was recently fixed. Unfortunately, this vulnerability is very easy to exploit by attackers with local access, resulting in trivial privilege escalation. This vulnerability affects many unsupported Linux distributions that are end-of-life. This adds additional pressure on security and vulnerability management teams struggling to eliminate unsupported and unpatchable software.

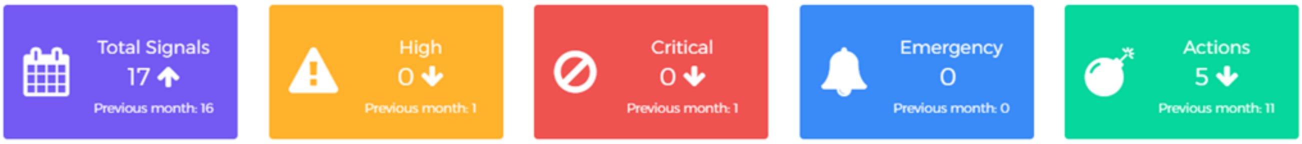
At a glance

The Log4Shell set of vulnerabilities have not resulted in mass exploitation as feared. This could be down to a concerted effort by all in responding to the imminent threat or the flaw itself is more suited to targeted attacks.

OVERVIEW

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

We welcome any inputs our readers may have about what kind of data may be useful in this part of the report.



Total Signals
17 ↑
Previous month: 16

High
0 ↓
Previous month: 1

Critical
0 ↓
Previous month: 1

Emergency
0
Previous month: 0

Actions
5 ↓
Previous month: 11

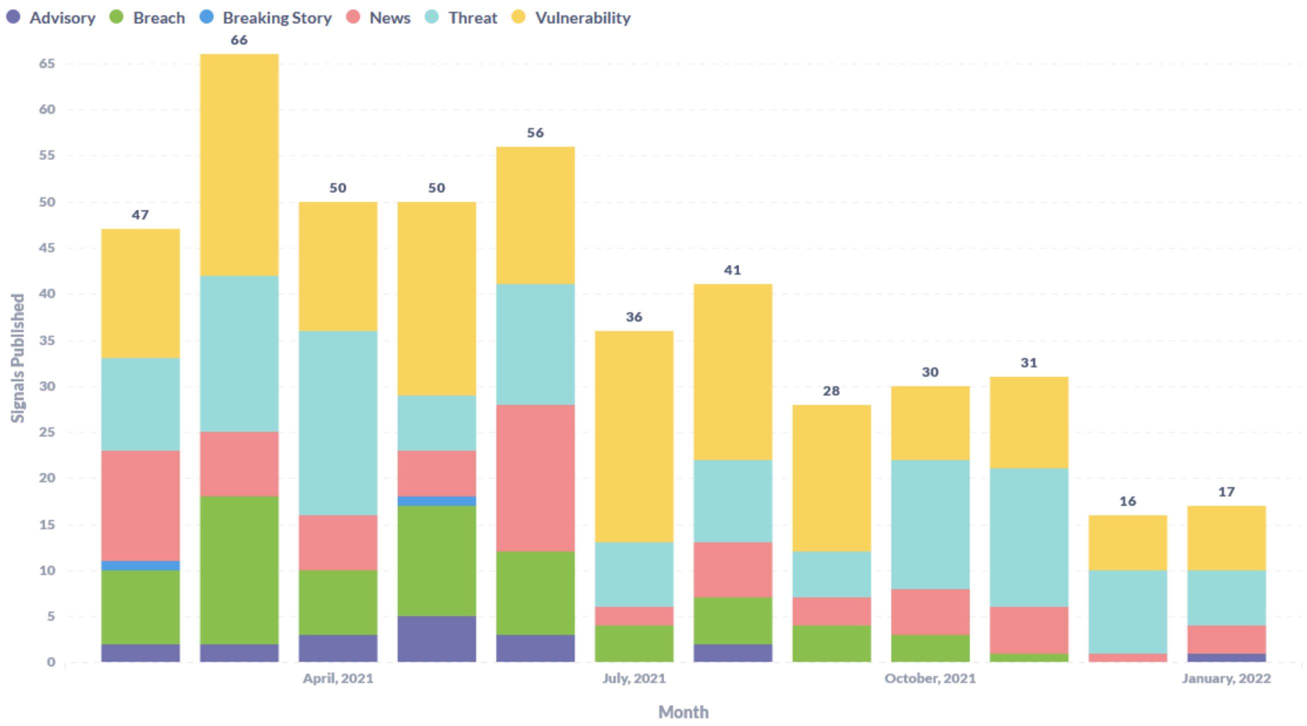
Signals Summary for January 2022

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.

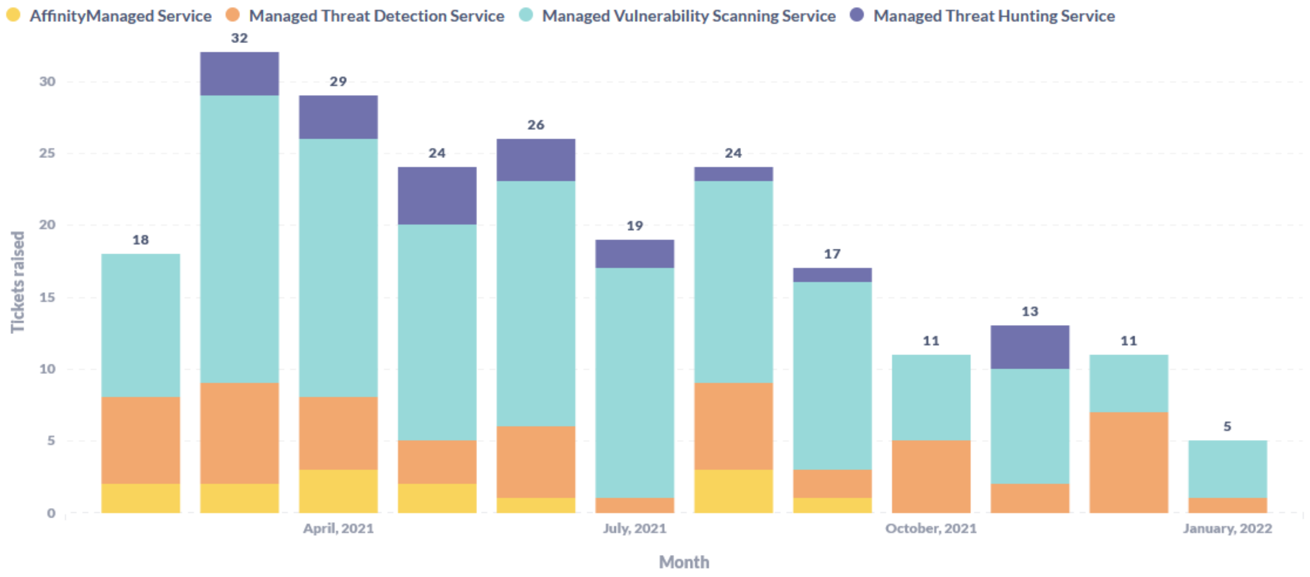
Categories – Monthly Breakdown



The distribution of signals across 2021 is tapering downward. December 2021 and January 2022 show similar figures, which could be the new baseline. As with the previous month, January 2022 shows clear favouritism toward vulnerabilities and threats.

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.

Services Affected



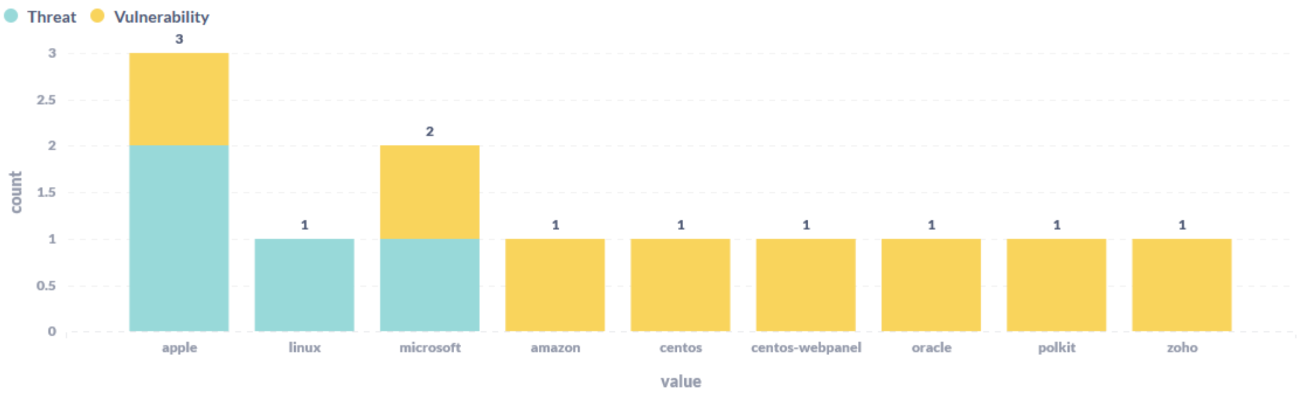
Tickets logged with our operations teams over the last 12 months

We are committed to ensuring that we take whatever action we reasonably can on behalf of our customers in response to the threats or vulnerabilities we describe in our advisories. To achieve this the research team raises specific action requests with each of our relevant operational units – Scanning, Threat Detection, Threat Hunting or the SOC. Customers who consume any of these services with us will then be contacted by the relevant team with advice on how their systems are impacted if necessary.

These action requests are recorded by our system and the number of requests raised per month since the over the past 12 months are reflected on the graph above.

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.

Technologies Affected



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

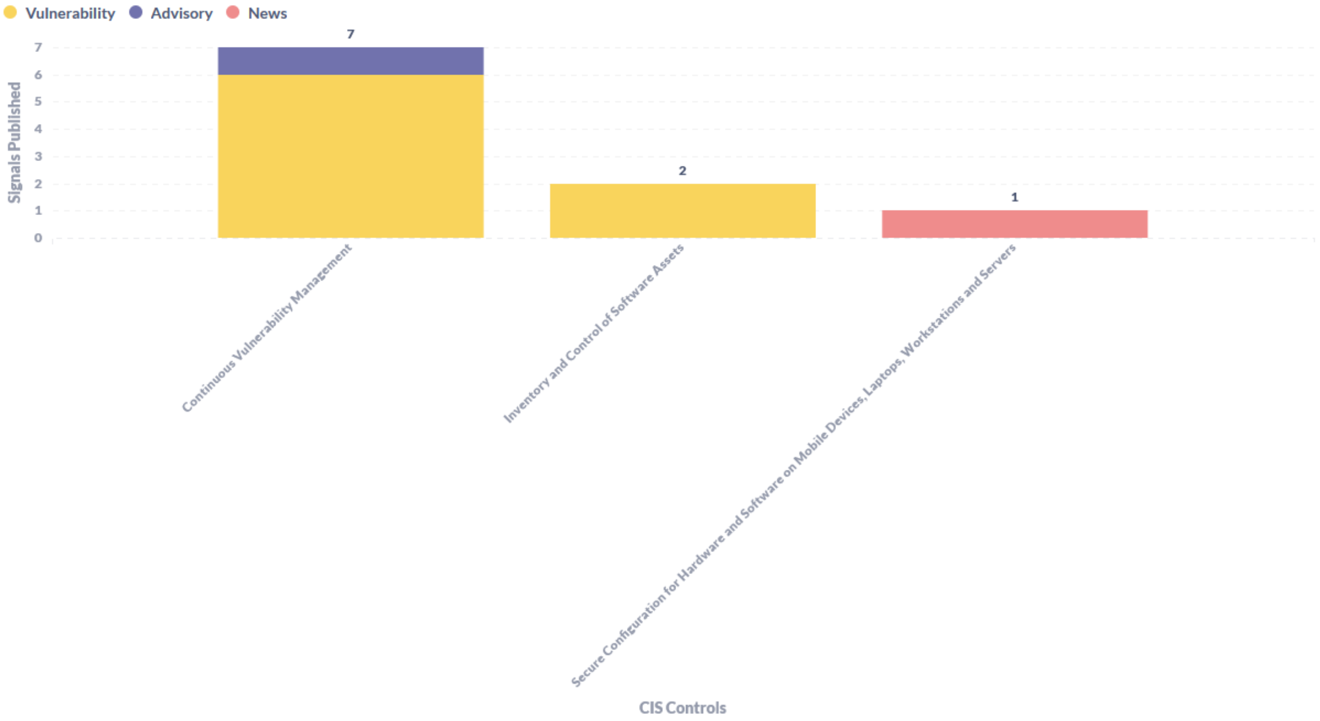
This month is interesting in that Linux and Apple (macOS) were featured in the same signal relating to a common threat. Apple fixed two zero-days that targeted its mobile operating systems, hence why Apple is overrepresented in this month's report.

Oracle released one of its largest quarterly patch updates that included fixes for the Log4J vulnerability identified as CVE-2021-44228.

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



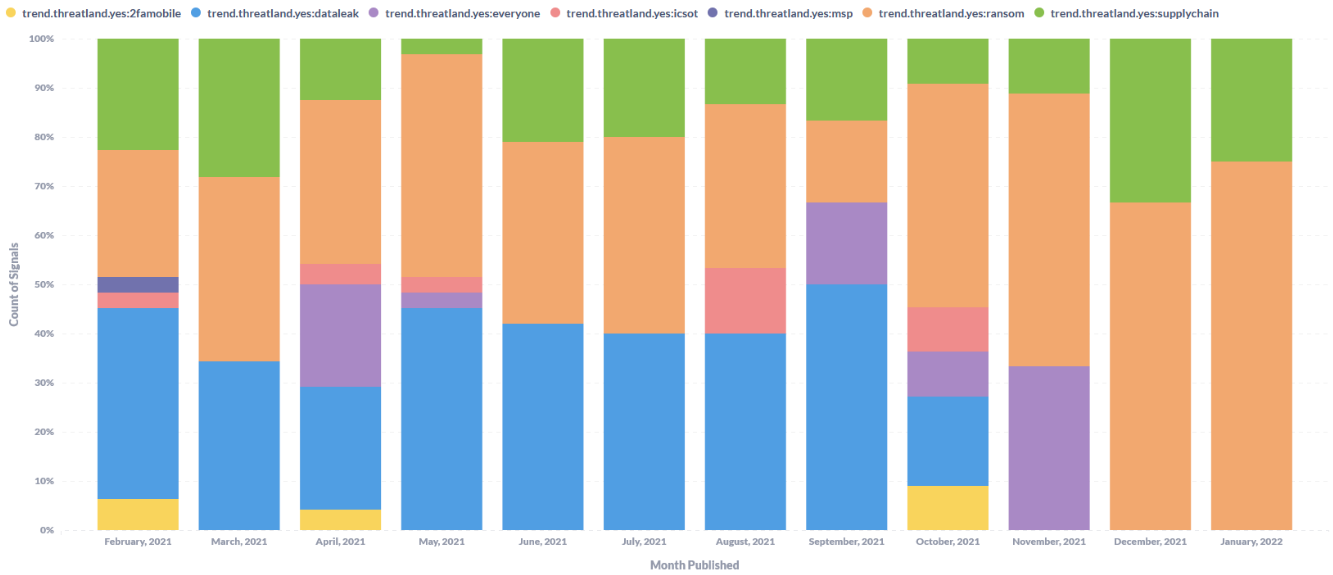
This chart summarises the recommendations our analysts have made in our Signals, separated between Threats and Vulnerabilities on the one hand, and the control failures we recognised in breaches, on the other.

As has been the clear pattern throughout the year, most of our recommendations fall under the basic CIS controls of Inventory and Vulnerability Management. The other two categories are also born out of the “Vulnerability Management” discussion.

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.



The topic that constantly gets mentioned in our Signals every month, for more than a year now, is ransomware. One surprising aspect of that is that the number of ransomware cases we observed is at its lowest point in more than a year. It is not clear why this is the case, and it is open to speculation at this point.

The ‘Supply Chain’ topic is once again noted this month courtesy of the Log4J vulnerabilities. It is unlikely that this issue will be solved. One of the subthemes here is the overdependence of technology companies on “free” Open-Source Software (OSS) with the assumption that the OSS code has been fully scrutinised for security bugs. OSS has a finite lifespan, and some tech companies use unsupported software for years. Any latent security issue here can be expensive to fix.

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 a new addition to our monthly report where we experiment with sharing ideas or observations of security researchers in the team. This view could be commentary 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.

Wicus

Ukraine-Russia Cyber Conflict

The situation between Russia and Ukraine is very tense and could change any minute. It is important for businesses to monitor the situation daily and adapt to new and relevant information as it becomes available. Businesses that have direct ties to other businesses in Ukraine need to be particularly vigilant.

We believe that businesses that have implemented a strong and tested response to the ransomware threat are well positioned to deal with any cyberattack that could potentially spill over as a result of aggression by Russia toward Ukraine. These controls will also help fend off other attackers that demonstrate capabilities and skills like that of groups associated with Russia.

Our primary recommendation involves developing and priming a robust Emergency- and Incident Response process, with trained people ready to execute it. If the threat level of this situation escalates, or more specific intelligence becomes available, the key will be to enact a swift response, possibly under very adverse circumstances. If or when a specific elevated threat emerges, this may take the form of a complete compromise, malware, ransomware, data destroying malware known as wiperware, data leak, DDoS, misinformation or disinformation campaign, an imminent threat or a vulnerability that needs to be patched. A response capability needs to be prepared to deal with any of the diverse situations listed above.

In addition, we recommend general defense-in-depth best practices for mitigating contemporary ransomware threats as a reasonable baseline for defense against a non-specific nation-grade attack.

Our comprehensive vendor-agnostic guide to defending against the threat of ransomware can be found at: https://orangecyberdefense.com/global/white-papers/beating-ransomware/.

Diana

Cyber-Extortionists suspiciously quiet in January 2022

Ransomware, or as we call it Cyber Extortion (Cy-X), has increased from 2020 to 2021, with a 34% increase in the number of victims being exposed and shamed on so-called ransomware leak sites. In Q4 2021, we saw volumes seen before only in Q3 and Q4 of 2020. That is why the January 2022 figures come as a surprise to us:

But in January '22 we observed a drop of 48% from the previous month in the number of victims being posted on the leak sites, and a 33% decrease of threat actor participation. There are two possible explanations for this trend.

The first most obvious explanation might be that after such a busy Q4, malicious threat actors needed a break as well and therefore extended their

Christmas leave after December. This is also supported by our data, if we look back in the leak volume of December 2020 (n=246) and January 2021 (n=135), we see a very similar trend. Forty-five percent fewer victims were recorded, and a decrease of 27% is also evident when comparing the unique threat actors that were active in December 2020 and January 2021. We could therefore say that our data is supporting this theory.

The second possible explanation could lie in the actions taken by the Russian FSB in mid-January 2022 in arresting some members of the REvil group. This came as a surprise since law enforcement actions taken by Russia within Russia have been very rare or non-existent to date. The arrests have not impacted the REvil cyber extortion operations per se, since the group had been inactive already since October 2021. But it could have had an impact on the 'fear of punishment' side, by suggesting to other cyber extortionists that their actions might have consequences. This explanation is of course highly dependent on Russia's strategy for diplomacy. Several news reports at the end of January described uncertainty and concerns on the part of threat actors involved in cyber extortion operations[1][2][3]. However, if we consider that the law enforcement action took place on the 14th of January and compare the activity before this date and after the 14th, we actually observe more victims posted after the 14th (n=58) than before the arrests (n=54).

We talk more about Russia and its Law Enforcement action in the next section.

Carl

Log4j still a thorn in the side

Whilst everyone is probably sick to death of hearing about the so called "Log4Shell" vulnerability in Apache Log4j, it is unlikely that it can be put to bed anytime soon and will likely remain a thorn in the side of defenders for some time. Indeed, the director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, referred to the vulnerability as "one of the most serious" she has seen in her entire career.

So, considering the sheer scope of this vulnerability, why did the predicted mass exploitations not happen? This was partly due to the almost unprecedented levels of cooperation and information sharing between enterprises, developers, security practitioners and government agencies. These joint efforts resulted in regularly updated indicators of compromise (IOC), mitigations and detection methods, as well as identifying vulnerable applications and other technical details about the vulnerability. However, whilst this work was being carried out by defenders, it is safe to say that threat actors were also carrying out similar work to try and find ways to

[1] https://intel471.com/blog/revil-ransomware-arrests-cybercrime-underground

[2] https://www.darkreading.com/threat-intelligence/revil-arrests-trigger-uncertainty-concern-in-cybercrime-forums

[3] https://cybernews.com/news/ransomware-affiliates-discuss-prison-life-amidst-revil-arrests/

weaponise the vulnerability, as part of the typical arms race between defenders and attackers trying to stay one step ahead of the other.

Obviously, some compromises did occur, resulting in systems being exploited to mine cryptocurrency, using lateral movement techniques to gain further access to networks or just to maintain persistence in an environment perhaps with a view to sell this access at a later date. Of course, there was no way that the prolific cyber extortion groups were going to pass up on this opportunity with the alleged Russia-based Conti group being the first to weaponise the vulnerability and use it in their chain of attacks.

The problem attackers faced was identifying targets and exploiting them with a predictable response coming back. With the Log4j library being the de facto standard for logging it was a safe bet that there would be some system inside a network running it, but there was no guarantee of getting a response back even if the exploit succeeded as the systems were not internet facing. One exception to this though was VMware Horizon access gateways, especially with more organisations having exposed instances to the internet to facilitate remote working due to the pandemic. This allowed attackers to target instances of VMware Horizon and get back a predictable response if the exploit was successful. The level of access an attacker could gain by compromising an instance of VMware Horizon certainly made it an even more valuable target.

The Log4Shell vulnerability has served to focus attention on how the use of free, open source, third party code in software can prove problematic, especially if it is not documented anywhere. In May 2021, President Biden issued an executive order on "Improving the Nation's Cybersecurity", a section of which covered Enhancing Software Supply Chain Security. One of the points in that section states that vendors should be "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website." In theory this should help organisations identify vulnerable instances in their environment if a vulnerability is announced in such a third-party piece of code as Log4j. It remains to be seen how quickly enterprises and developers get on board, however if customers start demanding this they may be left with no choice.

Hopefully, for defenders at least, the clamour around Log4Shell has now subsided. There are likely to still be some spikes of activity as and when new applications are found to be vulnerable but hopefully, they will be few and far between. It can be almost guaranteed though that threat actors will be looking for other vulnerable applications and also focusing attention on other widely adopted open-source libraries to see if they can be similarly abused.

Charl

Can the US government ‘enforce Zero Trust’, and will it make a difference?

https://www.scmagazine.com/analysis/compliance/dod-booz-allen-hamilton-to-develop-a-new-zero-trust-security-model

Subsequent to US President Biden’s May 12 Executive Order on Improving the Nation’s Cybersecurity, the article above describes how the US DoD plans to partner with Booz Allen Hamilton on a '$6.8 million project to prototype a new security model based on zero trust principles'.

This is almost certainly a positive move by the US Administration, and the planned 'upgrade' of their existing general-purpose security stack is no doubt a good idea.

But there's something to watch out for here: Zero Trust is a security design and operations *principle*, not a plug and play technology. In other words, the risk with this top-down approach to mandating the use of specific technologies, no matter how good the technology, is that security frequently fails in the execution, not in the design.

It would be a sad outcome if US government agencies replaced poorly deployed and administered technology with a new poorly deployed technology to check a compliance box, but failed to administer that any better.

Zero Trust is an emerging security paradigm in which all networks are considered equal, and untrusted, where there is no internal or external space, and where security must therefore be achieved on the endpoint and on the server without requiring a VPN. It's being adopted by leading thinkers like Google in their own security strategy, as well of course by vendors like Zscaler and Palo Alto.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred and requires an architecture that limits the 'blast radius' of a compromise on that basis.

Zero Trust is a design ideology, not a technology, but it does suggest some specific changes to the way we design remote access for our remote workers.

With Zero Trust the goal is to not connect users to a network but to the specific applications they are entitled to. We achieve that with a completely different design, where the secure connection no longer terminates on the network perimeter, but is proxied via an application-aware proxy that is hosted in the cloud. The proxy checks the user's identity and permissions and then connects them to the application in question, either in the cloud or using an on-premise gateway to facilitate a reverse-connection with a service in the internal network if required.

The immediate benefit is to reduce the impact of compromised credentials, as bad actors won't be able to navigate inside the entire network.

A second benefit of Zero Trust is the ability to make applications invisible on the internet, reducing the attack surface. Bad actors cannot attack what they can't see.

BUT, there are three important principles that the Zero Trust model teaches us:

- Apply the concept of least privilege.
- Assume that breach is inevitable or has likely already occurred.
- Every transaction must be authenticated and authorized.

Zero Trust principles are foundational and these are not negotiable. NIST SP800-207 lists seven such tenets [4]. Included in these are the requirement to always verify each transaction by verifying the authenticity of the transaction and whether the associated entity is authorized to issue the transaction. This principal acts like a barrier or perimeter that transactions must pass before being allowed to reach the intended service. Zero Trust Architecture must thus define its Identity, Credential and Access Management processes clearly.

These principles are easier to implement with a made-for-purpose technology, but the technology does not ensure that these principles are consistently applied.

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Good News Cyber

The aim of this section is to share news on events that can be considered positive, uplifting, or speak to progress in our industry.

One theme that we have repeated here is progress made by law enforcement in their fight against cybercrime. The Russian government arrested several individuals that they claim were affiliated with the REvil ransomware group. This action by the Russian government was rather surprising for some as Russia has for the most part turned a blind eye to cybercrime committed against businesses in nations other than Russia or the Commonwealth of Independent Sovereign nations, former eastern bloc members of the USSR. The timing is also interesting as the tension with the West increases considering the Russian military concentrating on the borders of Ukraine. We observed a decline in activity associated with REvil in the past four to five months, but other ransomware groups have benefited from REvil's absence.

In the second quarter of 2021 we published a Signal that explored an Executive Order issued by US President Joe Biding aimed at improving the cybersecurity of the Federal government. Efforts on this front has increased and recently the US Defense Information Systems Agency (DISA) awarded a multi-billion-dollar contract to security contractor Booz Allen Hamilton to develop a cybersecurity solution prototype dubbed "Thunderdome". This is to align with the zero trust requirements set out by the Executive Order and to test DISA's zero trust reference architecture. The project is set to leverage existing commercial technologies such as Secure Access Service Edge (SASE) and software defined networks (SDN). We are cautiously optimistic that the prototype will result in a valuable learning exercise into how to implement a sound security architecture using fresh thinking. The spirit of the Executive Order is to bolster and improve the cybersecurity of all agencies. Using technology purely for the sake of technologies sake without understanding the real problem contributes little. Technology vendors and consultants are incentivised to sell and bring in revenue. Convincing government to spend billions on tech solution that offers marginal benefits and lock the customer into yearlong support contracts does not align with the spirit. Gratuitous use of technology only makes matters worse as the attack surface is expanded and complexity is introduced. This need to be managed and the benefits are marginal.

MALWARE AND EXPLOITS

The cyber extortion threat, as with any cyber threat, is continuously evolving. This speaks to the motivation and drive of the attackers. It is not always clear what the real intent is of these attacks, but we can assume that monetary reward plays an important role for most cyber-criminal activity.

Operational security, in broad terms, refers to the steps that someone took to hide or obscure their actions while leaving very little to no evidence of their presence. This can backfire if someone does not pay attention, ultimately leaking important information that can be used to identify their operations. This was the case when an Indian based threat actor infected part of what looks like their own infrastructure. This was a boon for threat intelligences as it revealed a lot about this operation.

Malware authors have used programming languages such as C and C++ to create code that can be compiled to run on various operating systems. This is a type of efficiency gain that cuts down the development time and shares programming logic across multiple platforms. The developer must still be aware of the subtleties of the various platforms for the code to work as intended. C and C++ is notorious for being hard to port to other platforms. Modern programming languages such as Golang reduces the complexity of cross platform development. Programming in a modern language such as Golang can also yield productivity gains due to the rich eco systems of libraries that are automatically incorporated. Cross platform library support for C and C++ is limited.

New malware is also created to avoid detection and to fit in with the tactics, techniques, and procedures of a threat actor. Sometimes this is shared by particulars of their target. Needless to say, there will always be new malware.

Night Sky is the latest ransomware targeting corporate networks

Date: 10 January 2022

It's a new year, and with it comes a new ransomware to keep an eye on called 'Night Sky' that targets corporate networks and steals data in double-extortion attacks.

Indian Patchwork hacking group infects itself with remote access Trojan

Date: 11 January 2022

Researchers pounced on the opportunity the mistake created.

This new malware wants to create backdoors and targets Windows, Linux and macOS

Date: 13 January 2022

Researchers uncovered SysJoker when investigating another cyberattack - and warn that it's likely the work of an advanced hacking operation with the aim of espionage.

Microsoft says 'destructive malware' being used against Ukrainian organizations

Date: 18 January 2022

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

White Rabbit, a new ransomware possibly tied to APT group FIN8.

Date: 19 January 2022

Trend Micro analyzes a new ransomware called White Rabbit.

New DazzleSpy malware targets macOS users in watering hole attack

Date: 26 January 2022

A new watering hole attack has been discovered targeting macOS users and visitors of a pro-democracy radio station website in Hong Kong and infecting them with the DazzleSpy malware.

VULNERABILITY MANAGEMENT

The now infamous Log4Shell set of vulnerabilities saw many security teams scrambled during the closing weeks of 2021. This vulnerability has the potential to give attackers access to infrastructure buried deep in a network. For now, mass exploitation has not been observed. The storm surrounding this vulnerability has blown over, but it’s possible that future breaches could be linked to Log4J vulnerabilities.

Vulnerabilities in cloud platforms services are less common than traditional software but could impact more businesses if exploited. Two vulnerabilities were disclosed to AWS that could have resulted in customer data loss. Fortunately, these flaws were disclosed by ethical security practitioners.

Wormable vulnerabilities can be dangerous. This class of self-replicating software is normally associated with malicious intent and can spread rapidly in a network or across the Internet. A wormable exploit coupled with malware that allows remote access can give attackers unprecedented access, especially if the victims are numerous enterprise businesses. Microsoft released a fix for such a vulnerability in a component that is used to host web servers, such as IIS, on the Windows operating system. The nature of web servers mean that vulnerable services are possibly exposed to the Internet, making infection likely.

A serious vulnerability was disclosed that affects Linux distributions. This vulnerability has been hiding in a package called Polkit for years. It affects all Linux flavours running this software and could possibly result in an attacker with local access to escalate to maximum root level. Proof-of-concepts are circulating for this flaw and the reliability of the exploit puts a lot of pressure on teams to patch Linux hosts.

Apple’s mobile operating systems and Safari browser were found to contain serious vulnerabilities, of which one was exploited in the wild. Past stories included examples of how companies specialising in surveillance technology have used such flaws to facilitate spying on targets.

Microsoft: New critical Windows HTTP vulnerability is wormable

Date: 12 January 2022

Microsoft has patched a critical flaw tagged as wormable and found to impact the latest desktop and server Windows versions, including Windows 11 and Windows Server 2022.

Amazon Web Services fixes Superglue and BreakingFormation vulnerabilities

Date: 17 January 2022

Various AWS services have been vulnerable to security breaches that could have exposed AWS customer data.

Zoho patches new critical authentication bypass in Desktop Central

Date: 19 January 2022

Zoho has addressed a new critical severity vulnerability found to affect the company's Desktop Central and Desktop Central MSP unified endpoint management (UEM) solutions.

Almost 500 vulnerabilities fixed by Oracle in their latest quarterly Critical Patch Update

Date: 21 January 2022

Oracle released its Critical Patch Update fixing many vulnerabilities. Included in this are updates to several products impacted by the Log4J vulnerability.

Update on Log4J Vulnerabilities

Date: 21 January 2022

Log4j is an ubiquitous library maintained by the Apache Foundation and used by thousands of Java-based applications. On December 9th, a highly critical, easy to use, remote code authentication vulnerability now known as “log4shell” impacting most versions of the library was publicly disclosed. Exploitation attempts leveraging the flaw started happening a few hours later all over the world. Hundreds of open source and commercial products vulnerable to this flaw quickly started releasing security updates to address the issue numbered CVE-2021-44228 and first fixed by Apache in version 2.15. But additional lower risk vulnerabilities were found since and fixed in later Log4j versions.

Linux Servers at Risk of RCE Due to Critical CWP Bugs

Date: 26 January 2022

The two flaws in Control Web Panel – a popular web hosting management software used by 200K+ servers – allow code execution as root on Linux servers.

Linux system service bug gives you root on every major distro

Date: 27 January 2022

A vulnerability in the pkexec component that is present in the default configuration of all major Linux distributions can be exploited to gain full root privileges on the system, researchers warn today.

Apple Fixes 2 Zero-Day Security Bugs, One Exploited in the Wild

Date: 28 January 2022

iOS 15.3 & iPadOS 15.3 fix the Safari browser flaw that could have spilled users' browsing data, plus a zero day IOMobileFrameBuffer bug exploited in the wild.

NOTEWORTHY

A Swiss tech firm helped governments spy on users

Date: 09 December 2021

Mitto AG, a Swiss tech firm specialized in providing automated text messages for security codes, working with big companies such as Twitter, Telegram, LinkedIn, and Google, is accused of helping governments secretly spy and track the location of mobile phones. These allegations have been revealed by former employees of the company.

Drive-by RCE in Windows 10 discovered by Positive Security

Date: 13 December 2021

A drive-by remote code execution (RCE) vulnerability in Windows 10 and 11 that can be triggered simply by clicking a malicious URL has been identified last March by Positive Security researchers. Exploiting this flaw could allow an attacker to gain full access to a victim’s files and data.