





Security Intelligence

Quarterly Report

March 2022



Unrestricted



CONTENTS

CONTENTS	2
INTRODUCTION	3
OVERVIEW	4
Categories – Monthly Breakdown	5
Services Affected.....	6
Technologies Affected.....	7
Our Recommendations.....	8
General Trends	9
Cyber Extortion Trends in Q1 2022	9
Editor’s Notes (Beta)	14
OT/ICS Threats joining the mainstream, and that could mean trouble.....	14
Infiltrating Satellite Intranet Like (G)RU	16
Good News Cyber	18
DATA BREACHES	21
LAPSUS\$ group claims to have obtained internal access to OKTA.....	21
MALWARE AND EXPLOITS	22
BazarLoader operators now use contact forms to initiate contact.....	22
New RaaS LokiLocker targets Windows systems.....	22
New threat actor UNC2891 uses the same tools as LightBasin (UNC1945)	22
French companies targeted by Serpent backdoor according to ProofPoint.....	22
Trickbot adjourned, but used infected MikroTik routers as C2 proxies.....	22
New macOS variant of Gimmick malware deployed by Chinese Storm Cloud APT	22
Unknown Chinese threat actor targets Southeast Asia in Operation Dragon Castling	22
VULNERABILITY MANAGEMENT	23
Mozilla Firefox 97.0.2 fixes two actively exploited zero-day bugs.....	23
Bug in the Linux Kernel Allows Privilege Escalation, Container Escape.....	23
Microsoft Addresses 3 Zero-Days & 3 Critical Bugs for March Patch Tuesday	23
High severity DoS vulnerability fixed in OpenSSL.....	23
MFA misconfiguration and PrintNightmare vulnerability exploited by Russian hackers to breach an NGO	23
A vulnerability detected in the CRI-O container engine for Kubernetes	23
Public Redis exploit used by malware gang to grow botnet	23
Critical SonicWall firewall patch not released for all devices	23
New Spring Java framework zero-day allows remote code execution.....	23

INTRODUCTION

The war against Ukraine continues to dominate the news for obvious reasons. As well as the kinetic war cyber warfare activities are also being carried out by both sides. Different wiper malware has been detected targeting both Russia & Ukraine networks. Various “hactivist” groups supporting Ukraine have also been targeting Russian entities. This includes the hacking group “Anonymous” who breached and leaked the data of the Russian Central Bank. For their part the Ukrainian military intelligence service (GUR) leaked online the alleged personal data of 620 FSB employees. Thus far however the feared overspill of cyber attacks to other entities not directly involved in the war has not occurred, however everyone should remain vigilant for anything suspicious.

Okta, a major provider of authentication services and Identity and Access Management (IAM) solutions, suffered a data breach after the Lapsus\$ gang compromised a third-party support agents’ machine. Whilst the breach was not as severe as Lapsus\$ had hyped it up to be, Okta did themselves no favours in the way they initially handled and responded to the incident.

Vulnerabilities in security solutions reared their head again this month, with Sophos and SonicWall both disclosing critical remote code execution vulnerabilities in their firewall solutions. Given their purpose and level of access these deployed solutions enjoy, it is obviously imperative that access to these solutions is restricted and security patches prioritised and applied in a timely manner.

The OpenSSL encryption toolkit was found to be vulnerable to a high severity denial of service attack. The flaw occurs when parsing certificates containing public keys in compressed form or elliptic curve parameters explicit with a base point encoded in compressed form. Any vendors or developers using the OpenSSL library will therefore need to update their software to use the fixed version and release updated versions of their software.

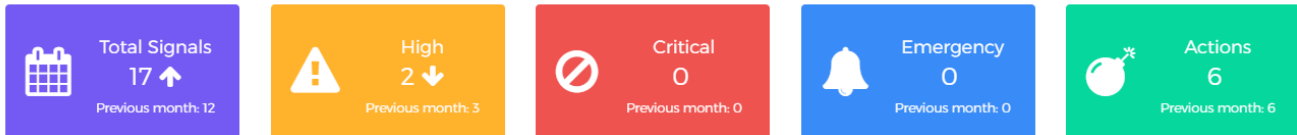
At a glance

Unfortunately, there seems to be no end in sight to the war against Ukraine. However, thus far the feared overspill of cyber attacks to other entities not directly involved in the war has not occurred, however everyone should still remain vigilant.

OVERVIEW

In this new beta 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...

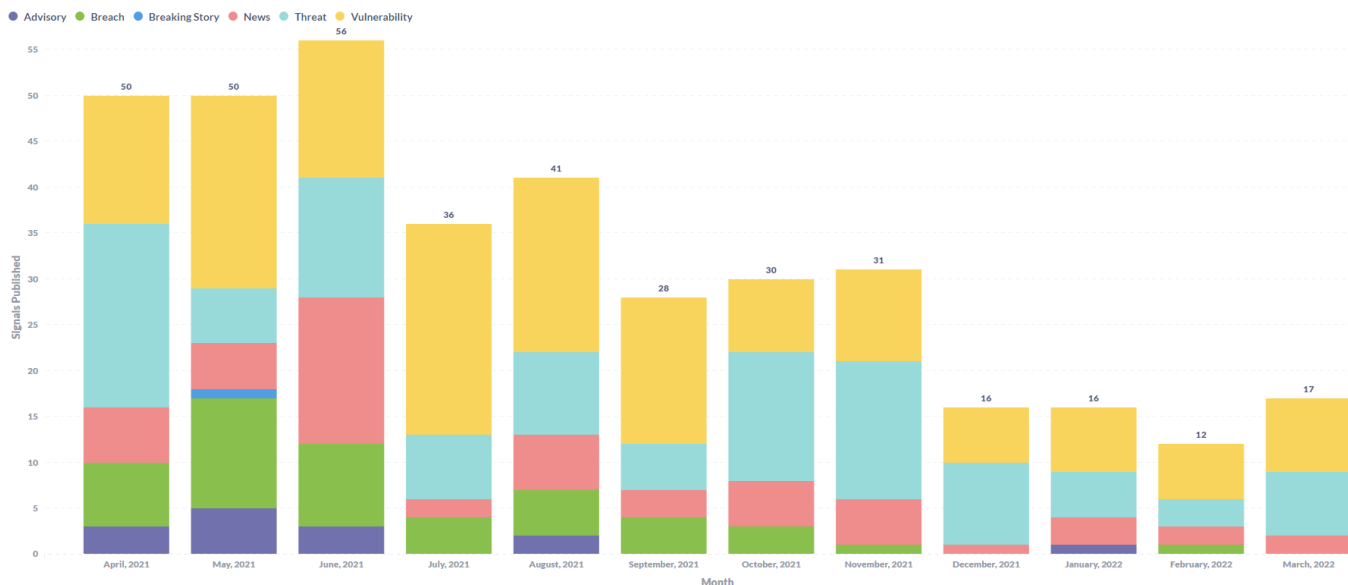


As stated previously, the number of total Signals published has been in decline for the past few months, although there was a slight uptick this month. This is not an indication that the number of threats or incidents have decreased but has been brought on by a change in the Signals service itself. Work has now been completed to transition the Signals service which is now branded as World Watch and delivered by the Orange Cyberdefense CERT. This also means that future versions of this report will likely be in a different form with different content.

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.

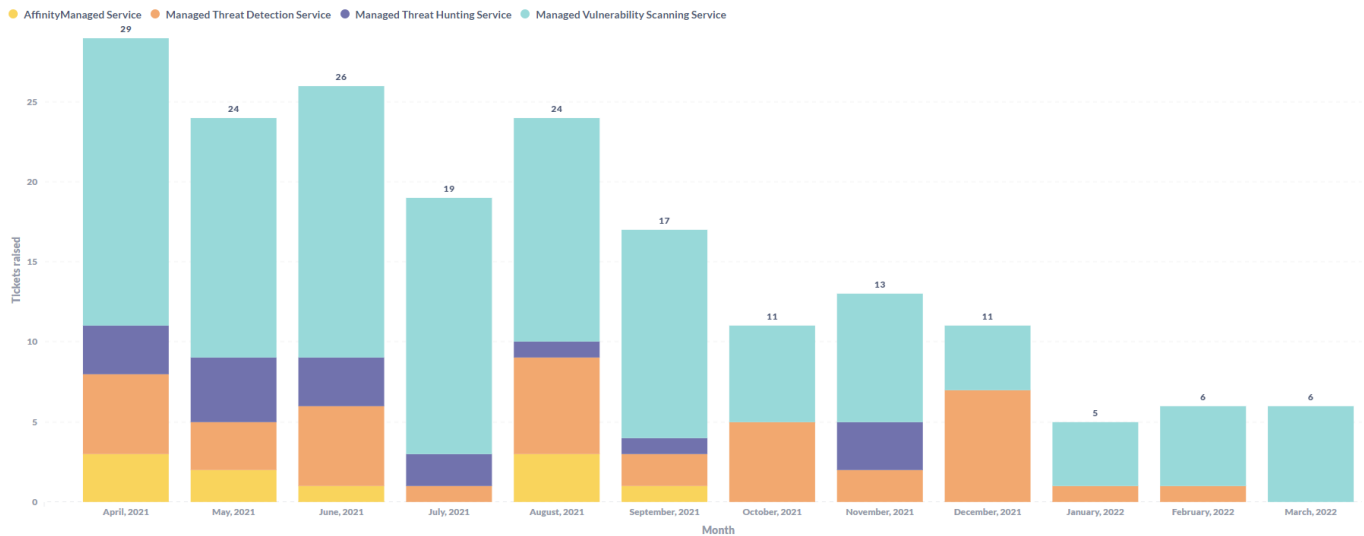
Categories – Monthly Breakdown



The distribution of Signals across 2021 is tapering downward. The past four 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.

Services Affected

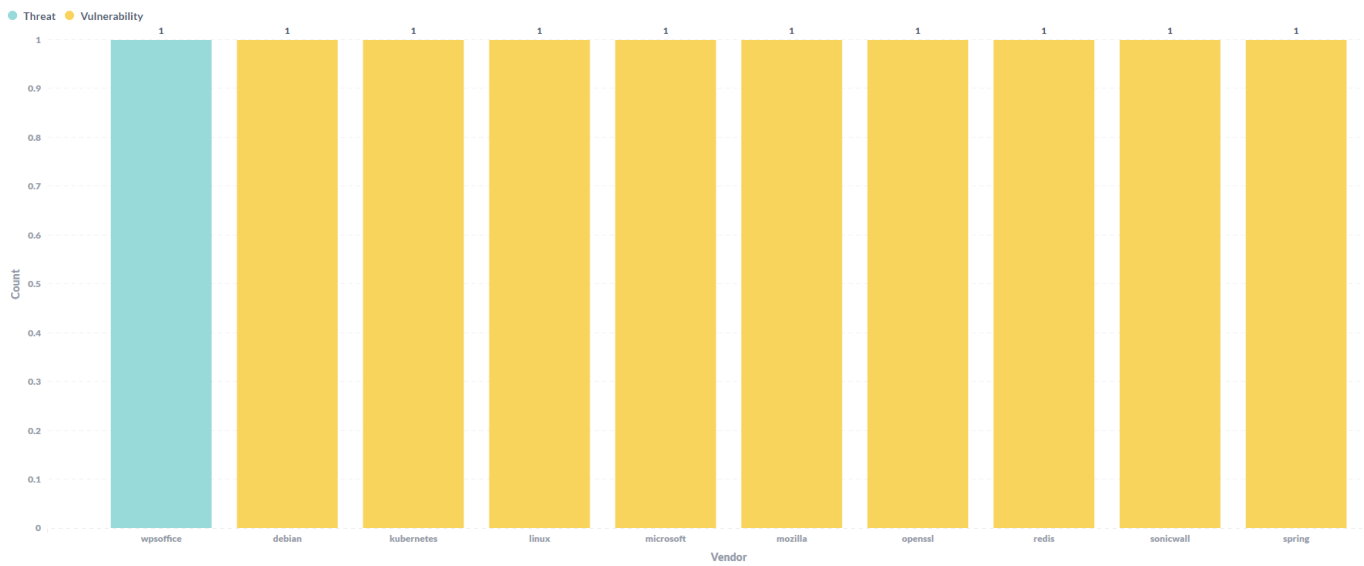


We are committed to ensuring that we take whatever action we reasonably can on behalf of our customers in response to the threats or vulnerabilities we describe in our advisories. To achieve this the research team raises specific action requests with each of our relevant operational units – Scanning, 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

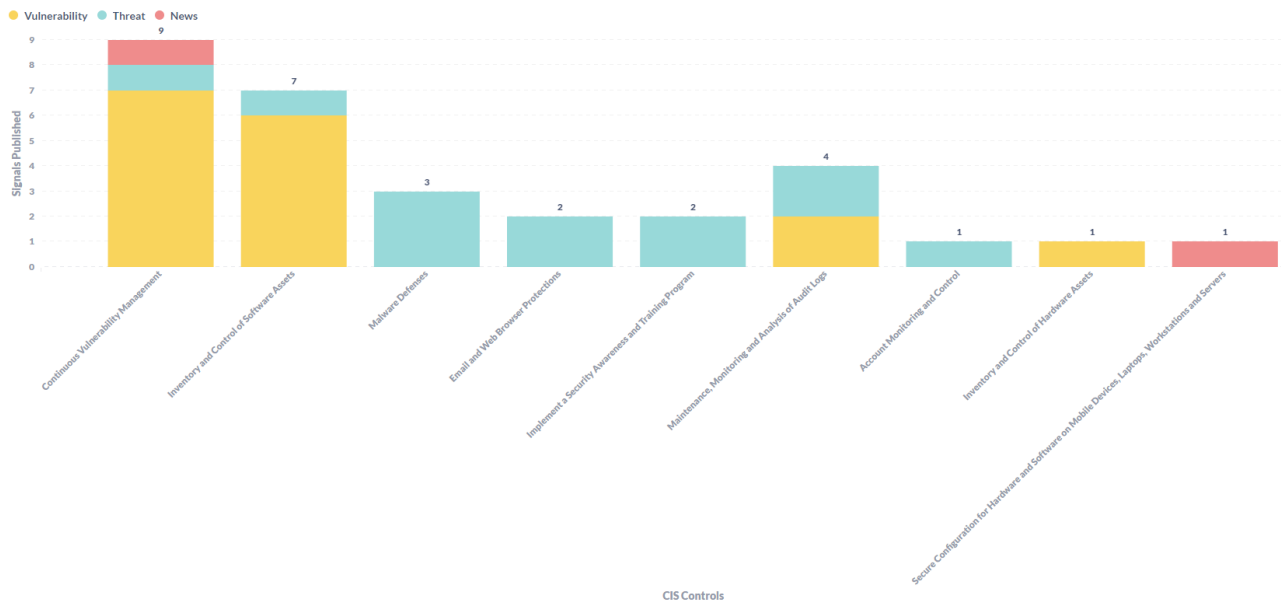


The chart above summarises the technology vendors that were referenced in our Signals across the various categories this month.

Microsoft is an obvious constant in this report due to their monthly Patch Tuesday releases. However, the presence of diverse technologies such as Kubernetes, Redis & Spring should serve to highlight just how broad the attack surface can be along with the difficulties still experienced with vulnerability management.

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

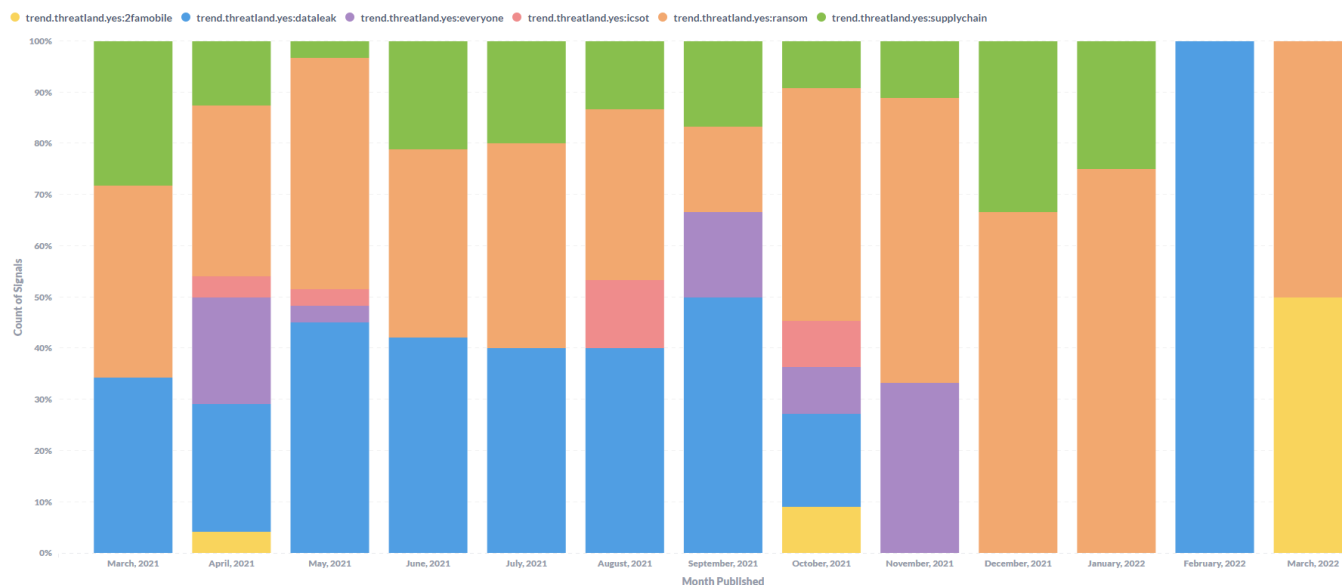


This chart summarises the recommendations our analysts have made in our Signals, separated between Threats and Vulnerabilities on the one hand, and the control failures we recognised in breaches, on the other.

As has been the clear pattern throughout the year, most of our recommendations fall under the basic CIS controls of Inventory and Vulnerability Management. This month though the Maintenance, Monitoring and Analysis of Audit Logs along with Malware Defenses controls make an appearance also signifying the increasing need to have robust threat detection processes in place.

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 Ransomware, or Cy-X, trend re-appeared again in March 2022, this is despite some successful law enforcement activities which disrupted some of the different gang's activities but in turn it appears the gangs were quickly able to recover. Making an appearance for the first time in a while is the 2famobile trend due to the breach of Okta. Whilst MFA and 2FA solutions should be a required piece of any security strategy, this will likely serve to put a bigger target on the solution provider's backs for attackers.

Cyber Extortion Trends in Q1 2022

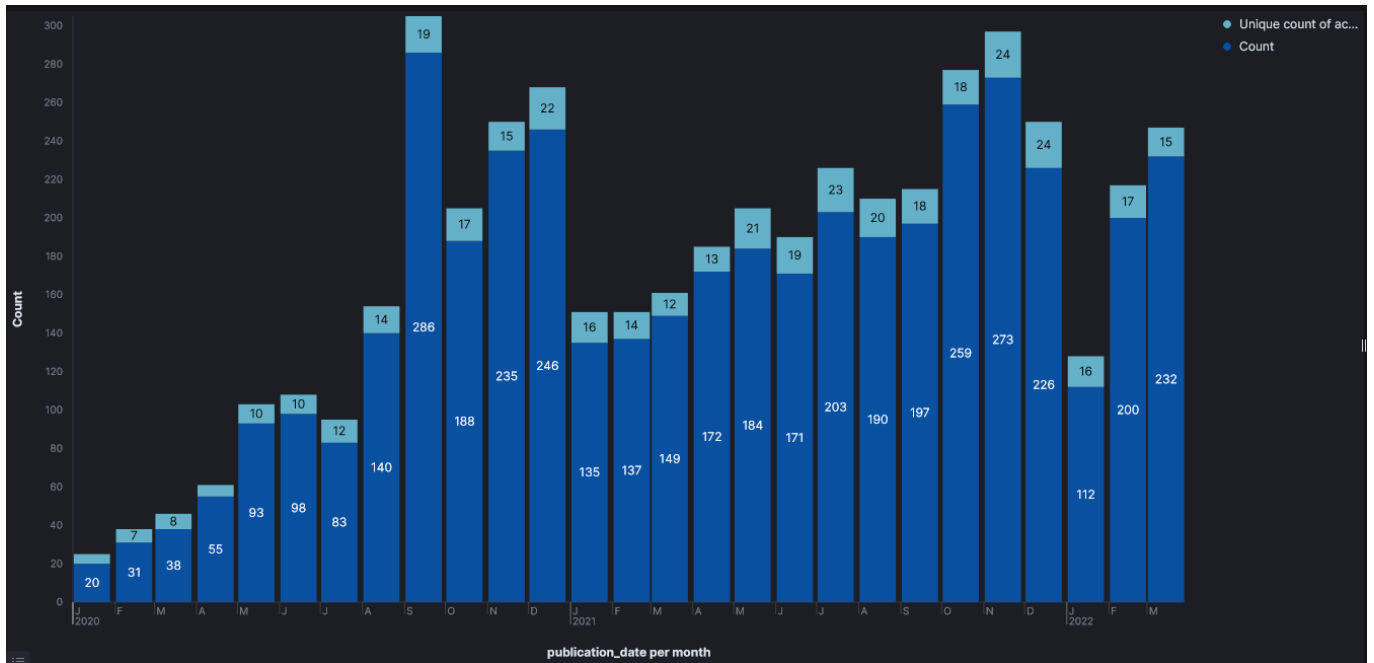
Summary

- We recorded 544 new extortion leaks on ransomware leak sites during Q1
- In Q1, we saw an increase of 29% in comparison to the year before (Q1 2021, n=421)
- The top 5 cyber ransomware cyber extortion groups contributing to Q1 2022 victims are: LockBit2 (41%), Conti (19%), ALPHV (aka BlackCat) with 8%, HiveLeaks (7%), Snatch (4%) and Others (21%).
- During Q1, some of the infamous REvil ransomware group members were arrested, and Conti experienced one of the biggest internal breaches, known as the 'Conti leaks'.
- We see less victims from the U.S., in March 2022 only 37,5% of all victims were from the U.S.

General Trends

During Q1, we collected 544 victims off the so-called ransomware leak sites. In comparison to the previous quarter, we see a decrease of 28% (Q4 2021, n=758). One reason for this is that historically, Q3 and Q4 are very busy quarters in terms of ransomware victimizations. While the beginning of the year has typically started very slow in the past two years of our ransomware monitoring. An additional reason might be the arrest of the majority of the REvil ransomware group members by the Russian FSB. The law enforcement action taken seemed to have had some impact on the overall extortion activity in

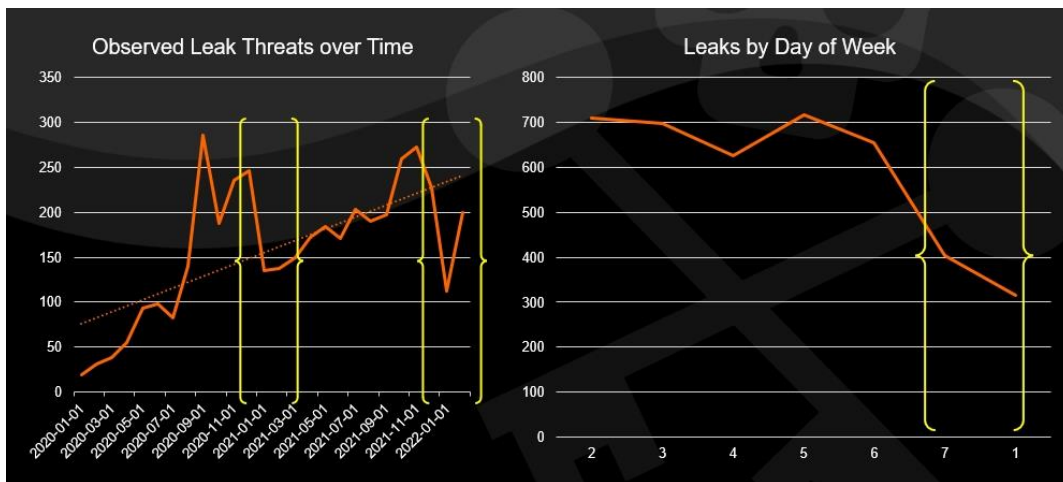
January. But already in February, extortion victims reached 'normal' levels of 200 victims per month, only to continue to 232 extortion victims in March.



Extortion incidents & unique threat actor count recorded from 2020 to March 2022 (n=4,353)

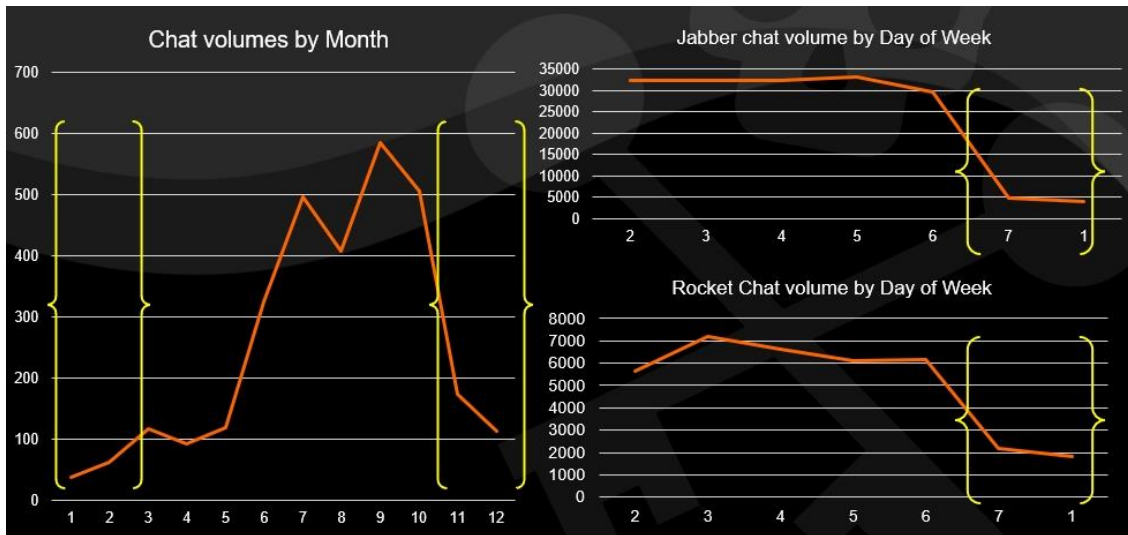
Threat actor activity – business hours

At the end of February, Russia began the war against Ukraine; and one of the most active extortion groups, namely Conti, expressed their support for the Russian government. Consequently, they experienced one of the biggest internal leaks that any extortion operation has seen so far. Within a few days, hundreds of thousands chat messages were publicly leaked. At the time of writing, we are still analyzing all the material. After initial analysis, what we noticed in terms of activity is that no matter how sophisticated the threat actors are, at the end they are just humans, working close to normal business hours. We are collecting external threat data from the ransomware leak sites and thus have a time stamp when they were posted as well as now the internal chat activity. This provides us with a good picture on the time of the day and which day of the week the threat actors are active, as can be seen below.



External leaks on ransomware leak sites showing months of the year and day of the week

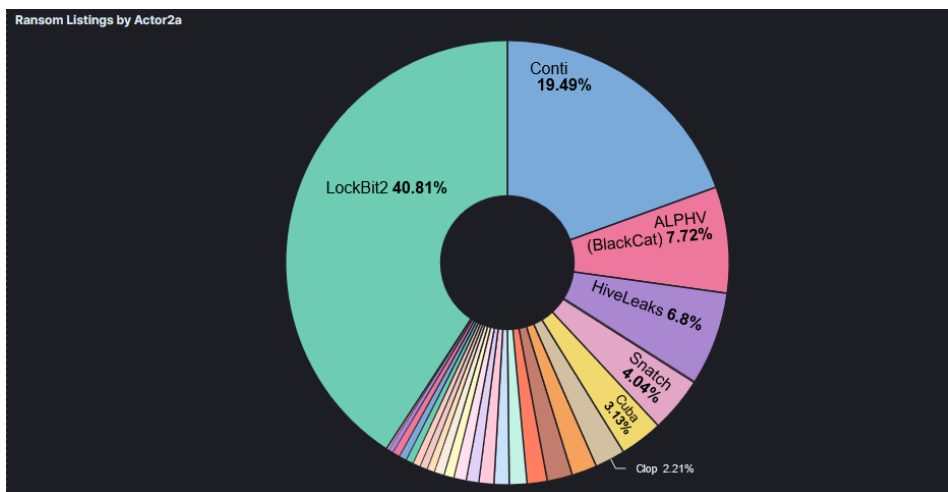
The external leak sites data shows us that we do not observe threat actors being very active during major holidays seasons such as Christmas, New Year’s Eve and winter vacation in February. When looking at the day of the week, we can see that ‘7’ representing Saturday and ‘1’ representing Sunday show the least activity and thus there seems to be a Monday to Friday work mentality. We observe very similar patterns from the internal chats from Conti. There is not as much activity during the above-mentioned holiday season as well as very low activity during the weekends.



External leaks on ransomware leak sites showing months of the year 2021 and day of the week

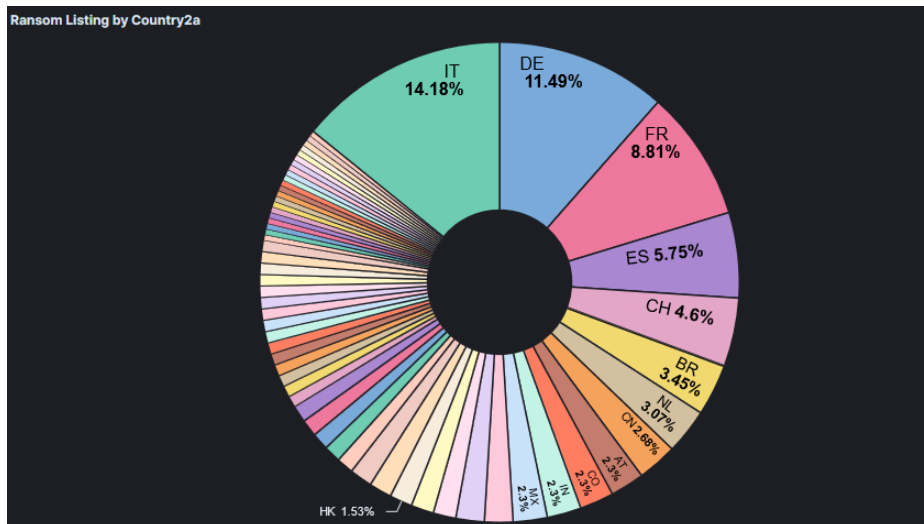
Victimology of Q1 2022

Despite the rapid increase of leaks from January till March 2022; we see some other patterns worthwhile pointing out. First of all, threat actors that have contributed to the Q1 2022 victimology have only changed slightly. We still observe LockBit 2.0 as number one contributor with 41%; followed by Conti (19%), both have been the two most active groups for the past 9 months. The other threat actor groups that have contributed to the Q1 2022 victim organizations were: ALPHV (aka BlackCat) with 8%, HiveLeaks (7%), Snatch (4%) and Others (21%).



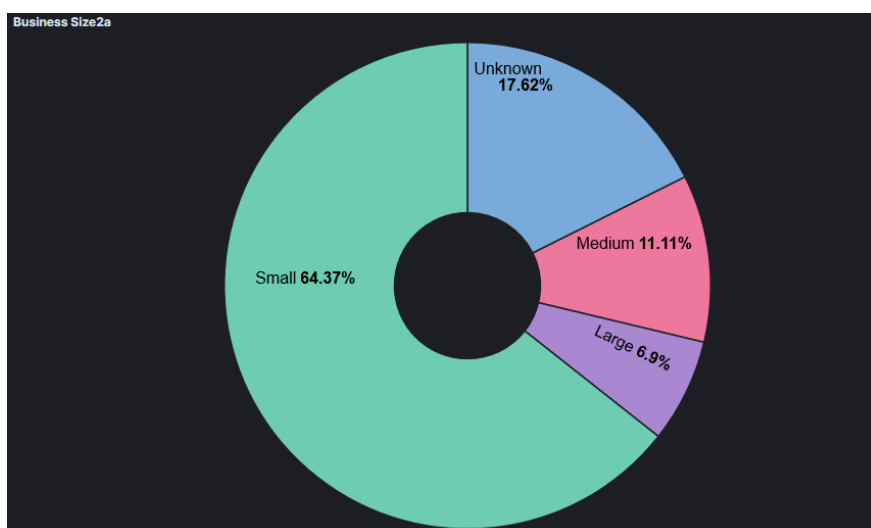
Contributors to cyber extortion leaks in Q1 2022

Countries in which the victims are headquartered have changed over the past months. We see a very visible decrease in U.S. based victim organizations and observe more victims from other regions such as non-English speaking European countries (e.g. Italy, Germany, France, Spain), but also Asia (e.g. China) and South America (e.g. Brazil, Columbia).



Victim organization’s country excluding US, GB & CA in Q1 2022

The Small businesses remains the most impacted business size for Q1, which in our understanding are businesses with an employee count of 1 to 1000. 64% of all victim organizations belonged to the small business size, followed by medium sized businesses (employee count 1001 to 10,000) representing 11% of victims. Large organizations impacted represent 7% of victims, meaning 7% of all victim organizations were larger than 10,000 employee count. Approximately 18% of victims could not be classified as either small, medium, or large.



Business size impacted by cyber extortion in Q1 2022

And lastly, despite seeing the most victims in March 2022 during Q1, we observed a decrease in the number of threat actors contributing to the victim count for March, thus showing us proportionally the lowest number of threat actors (n=15) but the highest count of victims (n=232) in Q1.

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.



Charl

OT/ICS Threats joining the mainstream, and that could mean trouble

In an April 14 World Watch security advisory, we discussed a joint report released by CISA, NSA, FBI, and the Department of Energy (DOE), warning of a new Industrial Control Systems (ICS)-focused malware toolkit called 'Pipedream', which can hijack multiple different kinds of industrial devices. The initial analysis of the malware was performed by security firm Dragos, but Mandiant are also tracking it and report that it represents "an exceptionally rare and dangerous cyberattack capability".

The malware itself is fascinating and powerful, as is described in the CISA advisory¹, which is well worth the read.

More interesting to me, however, is that this is perhaps only the seventh ICS-focused malware of this kind ever reported. When we say 'ICS-focused' in this context, we mean that the malware directly targets and attacks the actual industrial system control technologies, like PLCs for example, rather than just the traditional (Windows) IT systems that are typically used for programming, monitoring, and management. This is an important distinction.

I think this heralds a brewing storm, created from the convergence of three systemic factors:

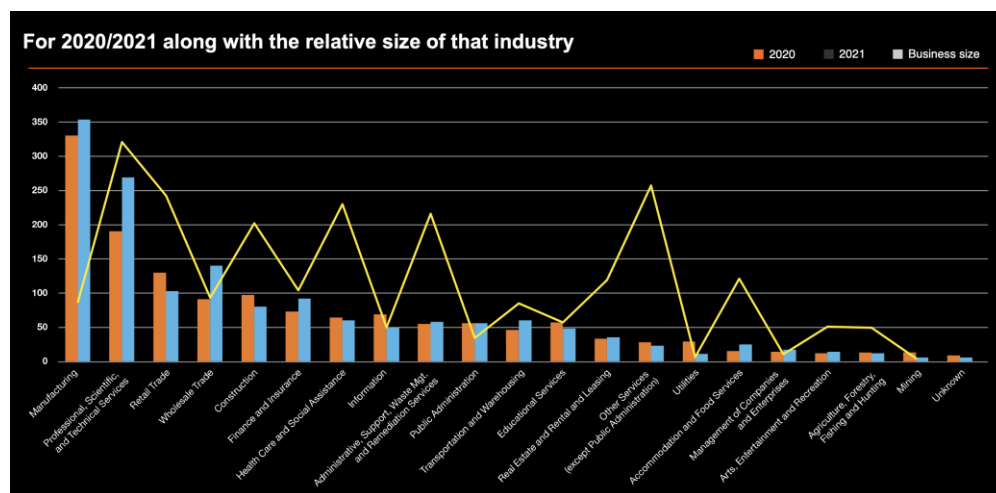
1. As this new malware indicates, state actors are clearly making significant investments into this kind of capability. History teaches us that this kind of government investment (which is often financed from massive 'national security' budgets' can be the 'rising tide that floats all boats' in the offensive security domain. Simply put, these kinds of state-developed capabilities are never restricted to the 'government' domain and inevitably have the effect of inflating the threat for everyone concerned
2. Recent reports² reveal that Ukrainian defenders had thwarted a Russian cyberattack on Ukraine's power grid that could have knocked out power to two million people. This would not have been the first such attack against Ukrainian power systems, and similar attacks in the past have succeeded. This is a powerful reminder that malicious actors are not only improving their technical capabilities; they are also willing and able to bring those capabilities to bare in actual assaults on industrial system. Similarly, as Wicus describes below, the successful attack against ViaSat is probably

¹ <https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>

² <https://www.bbc.com/news/technology-61085480>

one of the most ‘interesting’ and impactful cyber elements of the war thus far.

- The third worrying factor is that the Manufacturing sector appears to be very poorly positioned to defend itself, even against traditional IT threats like Ransomware and Cyber Extortion. As the chart below from our 2022 ‘Security Navigator’ report shows, confirmed Cyber Extortion incidents impact the Manufacturing sector at a rate completely disproportionate to the size of the vertical:



In the chart above we illustrate the number of victims per industry in our data set for equivalent periods in 2020 and 2021, alongside the estimated total number of businesses in that industry. Our data shows that over the last 12 months 23% of all Cyber Extortion victims are from this sector – more than 500 unique businesses.

We posit that this is not a function of attacker target selection, or industry size, but rather the general level of vulnerability of businesses in that sector. The level of vulnerability doesn’t predict who will be attacked, but rather which businesses, when attacked, will end up being leak threat victims. From further analysis of this data, we note that the top actors are all compromising the most victims in the same few industries – the same industries that fall victim most often over-all. If actors were targeting specific industries, we’d expect to see at least some level of specialization. The fact that we don’t, suggests that these most-featured industries are not being specifically targeted, but rather have something else in common. We propose that the common denominator is simply that they are less prepared to stave off attacks.

The combination of these three converging factors suggests that businesses in the Manufacturing sector, especially those that rely on Industrial Control Systems, could be in for a hard time in the months and years to come.



Wicus

Infiltrating Satellite Intranet Like (G)RU

Shortly after Russia invaded Ukraine, we learnt of a cyberattack affecting clients of Viasat's KA-SAT satellite service operating in the European region including Ukraine. The attack disabled several customer premise equipment (CPE) devices. These satellite 'modems' went dead for no apparent reason. At first some speculated that a remote code execution vulnerability could be to blame. A couple of weeks later we learned that attackers managed to overwrite the firmware of some of the modems, rendering the devices inoperative, requiring complete device replacement.

In a statement issued by Viasat, attackers managed to gain access to a specific management console associated with Satellites managed by a subsidiary Skylogic on behalf of Viasat. What was more astonishing was that the attackers gained access to this 'trusted management console'.

The malicious software update was delivered through the Skylogic management console using the existing over-the-air update mechanism. The malicious code damaged the firmware of the satellite CPEs, that in turn rendered the devices inoperable. Viasat had to ship replacement devices to affected customers. According to a report by The Record, one customer called Enercron lost remote access to over 5 800 wind turbines in Germany because of this attack.

The war in Ukraine is defining what modern warfare looks like and is, as expected, spilling over into cyberspace. Several malware strains attributed to attacks against Ukrainian government targets have been identified. One commonality or theme is that the malware tends to damage or destroy its targets as you would expect a bomb or munition used in a war would do. In the case of Viacom or Skylogic for that matter, it's how it was delivered that is disconcerting.

How did the attackers gain access to the management console? Viacom said in its statement that a 'misconfigured VPN appliance' was exploited and then used by the attackers to gain entry to its networks. From there the attackers snaked their way through the network until they reached the 'trusted management network' segment.

The title of this section makes a bold claim or assumption, namely that this attack is attributed to Russia. Officially there is no public attribution at the time of writing. SentinelOne offered a hypothesis speculating that the malware responsible for wiping the satellite firmware, called AcidRain, has links to another piece of malware called VPNFilter. The attribution by FBI, NSA, and CISA of VPNFilter and associated Cyclops Blink malware to Russia's General Staff Main Intelligence Directorate (GRU) thus indirectly suggests that AcidRain has a potential link to

GRU. Original analysis of the VPNFilter malware was first made public by Cisco Talos in 2018 and involved malware that infected MikroTik routers.

I was in the audience when Orange Tsai and Meh Chang delivered their 'Infiltrating Corporate Intranet Like NSA - Pre-auth RCE on Leading SSL VPNs' talk at Black Hat USA 2019. Ever since this talk, it feels like we have seen a dramatic increase in the number of cyberattacks reported that can be traced back to a VPN compromise. Now, this is possibly one of the vectors used as part of a war. It is likely that we will continue to read about compromised VPN appliances in the year to come.

Good News Cyber

Alleged members of the Lapsus\$ cyber extortion group were arrested by law enforcement shortly after the group claimed to have gained access to resources belonging to Identity and Access Management company Okta. Two teenagers were formally charged.

A U.S. court sentenced an Estonian man to 66 months in prison for involvement in 13 ransomware attacks. The damaged linked to these crimes are estimated at \$53 million.

The “Good News” below comes courtesy of a recent World Watch advisory published by the Orange Cyberdefense CERT team:

Multiple security improvements have recently been released by IT and Cloud providers. Below are a few of them:

Google Account

In a proactive effort to secure user accounts, in 2021 Google auto-enrolled over 150 million accounts in two-step verification. As a result of this initiative, the Mountain View company observed a 50% decrease in accounts being compromised among those users.

Microsoft Windows

On February 9, Microsoft announced in a documentation post that the Attack Surface Reduction rule "Block credential stealing from the Windows local security authority subsystem (lsass.exe)" will change from 'Not Configured' to 'Configured' and the default mode will be set to 'Block'. Under this new default configuration, the Local Security Authority Server Service (LSASS) process is protected against being opened and having its memory dumped by other processes, even ones with administrative privileges, making it harder for attackers to recover NTLM hashes from this service using programs such as Mimikatz.

On March 16, Microsoft released Windows Server Preview Build 25075. In this new version, the SMB server now implements a rate-limit of 2-second between each failed NTLM or PKU2U-base authentication. In practice, this change makes brute-forcing accounts against an accessible SMB server take hundreds of times longer.

Finally, on April 5, Microsoft announced Windows Autopatch to be released in July 2022. The feature will be available to Windows 10/11 Enterprise E3 customers. The Autopatch service works by automatically breaking the organization's device fleet into 4 rings:

- a 'test' ring, containing a minimum number of representative devices,
- a 'first' ring, containing 1% of devices,
- a 'fast' ring with 9% of devices,
- and a 'broad' ring for 90% of devices.

The population of these rings is managed automatically, but it is possible to move specific devices from one ring to another. Updates are installed in the 'test' ring devices first, and after a period of validation they progress to the next ring and so on. Autopatch monitors device performance and compares performance to pre-update metrics. Microsoft states that security updates are rolled out relatively fast, while feature updates are rolled out more slowly, with each ring being afforded 30 days so that users have an opportunity to report any issues that can't be detected automatically.

As announced in our previous update, Microsoft now allows App Installer for MSIX to be used again, since March 30. Administrators should update to the latest installer, also configure a specific policy, as explained in the update of their article [here](#).

GitHub

On April 4, GitHub announced a new push protection feature for its GitHub Advance Security service that allows blocking of push requests containing secrets such as access tokens, API keys or other credentials. GitHub Advance Security is currently only available for enterprise accounts.

GitHub also announced on April 6 the introduction of the "dependency review" action. When added to a repository, the action scans pull requests for dependency changes and checks if the new dependencies have existing vulnerabilities, raising an error to inform the user of the problem. This feature is available for all GitHub users.

DATA BREACHES

LAPSUS\$ group claims to have obtained internal access to OKTA

Date: 22 March 2022

Okta, a major provider of authentication services and Identity and Access Management (IAM) solutions, said it is investigating claims of a data breach after the Lapsus\$ gang stated they have access to Okta's systems.

MALWARE AND EXPLOITS

BazarLoader operators now use contact forms to initiate contact

Date: 16 March 2022

Upon investigating a recent BazarLoader phishing campaign, Abnormal Security researchers found that website contact forms were used by one threat actor to initiate communication with the targets. Once the target responds (sometimes automatically) to the unsolicited contact, from the perspective of an email system, the target company itself is initiating the communication with the attacker rather than the other way around, allowing malicious actors to circumvent some email defense mechanisms. After communication has been established with the victim, the attackers send another email with a link to a malicious file hosted on legitimate file sharing systems such as TransferNow or WeTransfer.

New RaaS LokiLocker targets Windows systems

Date: 18 March 2022

New Ransomware family LokiLocker discovered by BlackBerry researchers.

New threat actor UNC2891 uses the same tools as LightBasin (UNC1945)

Date: 22 March 2022

The LightBasin malicious actor may be associated with another actor tracked under the name UNC2891.

French companies targeted by Serpent backdoor according to ProofPoint

Date: 22 March 2022

A backdoor dubbed Serpent is being used by an unknown actor to target French companies.

Trickbot adjourned, but used infected MikroTik routers as C2 proxies

Date: 23 March 2022

Trickbot compromises MikroTik routers to act as proxies for C2 servers.

New macOS variant of Gimmick malware deployed by Chinese Storm Cloud APT

Date: 24 March 2022

A new macOS variant of the GIMMICK malware was discovered when deployed by Chinese Storm Cloud APT group.

Unknown Chinese threat actor targets Southeast Asia in Operation Dragon Castling

Date: 25 March 2022

A new operation tracked under the name Operation Dragon Castling is currently conducted by an unknown group but belonging to the large cluster of "Chinese APT groups". This campaign targets betting companies located in Southeast Asia and more specifically in Taiwan, the Philippines, and Hong Kong.

VULNERABILITY MANAGEMENT

Mozilla Firefox 97.0.2 fixes two actively exploited zero-day bugs

Date: 11 March 2022

Mozilla has released Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0, and Focus 97.3.0 to fix two critical zero-day vulnerabilities actively exploited in attacks.

Bug in the Linux Kernel Allows Privilege Escalation, Container Escape

Date: 11 March 2022

A missing check allows unprivileged attackers to escape containers and execute arbitrary commands in the kernel.

Microsoft Addresses 3 Zero-Days & 3 Critical Bugs for March Patch Tuesday

Date: 11 March 2022

The computing giant patched 71 security vulnerabilities in an uncharacteristically light scheduled update, including its first Xbox bug.

High severity DoS vulnerability fixed in OpenSSL

Date: 17 March 2022

The encryption toolkit providing an implementation of cryptographic algorithms and the SSL/TLS communication protocol identified as OpenSSL is vulnerable to a high severity bug. The flaw, identified as CVE-2022-0778, is related to certificate parsing and allows an attacker to realize a denial of service (DOS) attack. This vulnerability affects OpenSSL versions 1.0.2, 1.1.1 and 3.0 has been fixed with the release of versions 1.0.2zd (for premium support customers), 1.1.1n and 3.0.2. Version 1.1.0 is also impacted, but it is no longer supported and therefore will not receive a patch.

MFA misconfiguration and PrintNightmare vulnerability exploited by Russian hackers to breach an NGO

Date: 17 March 2022

The US FBI and CISA agencies released a joint advisory on March 15 warning that Russian state-sponsored threat actors last year compromised an NGO by exploiting a default vulnerable configuration of Cisco's Duo MFA solution and leveraging the "PrintNightmare" vulnerability.

A vulnerability detected in the CRI-O container engine for Kubernetes

Date: 18 March 2022

The CRI-O container engine for Kubernetes is vulnerable to a high severity bug allowing an attacker to execute arbitrary code under certain conditions.

Public Redis exploit used by malware gang to grow botnet

Date: 30 March 2022

Threat analysts report having spotted a change in the operations of the Muhstik threat group, which has now switched to actively exploiting a Lua sandbox escape flaw in Redis.

Critical SonicWall firewall patch not released for all devices

Date: 30 March 2022

Security hardware manufacturer SonicWall has fixed a critical vulnerability in the SonicOS security operating system that allows denial of service (DoS) attacks and could lead to remote code execution (RCE).

New Spring Java framework zero-day allows remote code execution

Date: 31 March 2022

A new zero-day vulnerability in the Spring Core Java framework called 'Spring4Shell' has been

publicly disclosed, allowing unauthenticated remote code execution on applications.