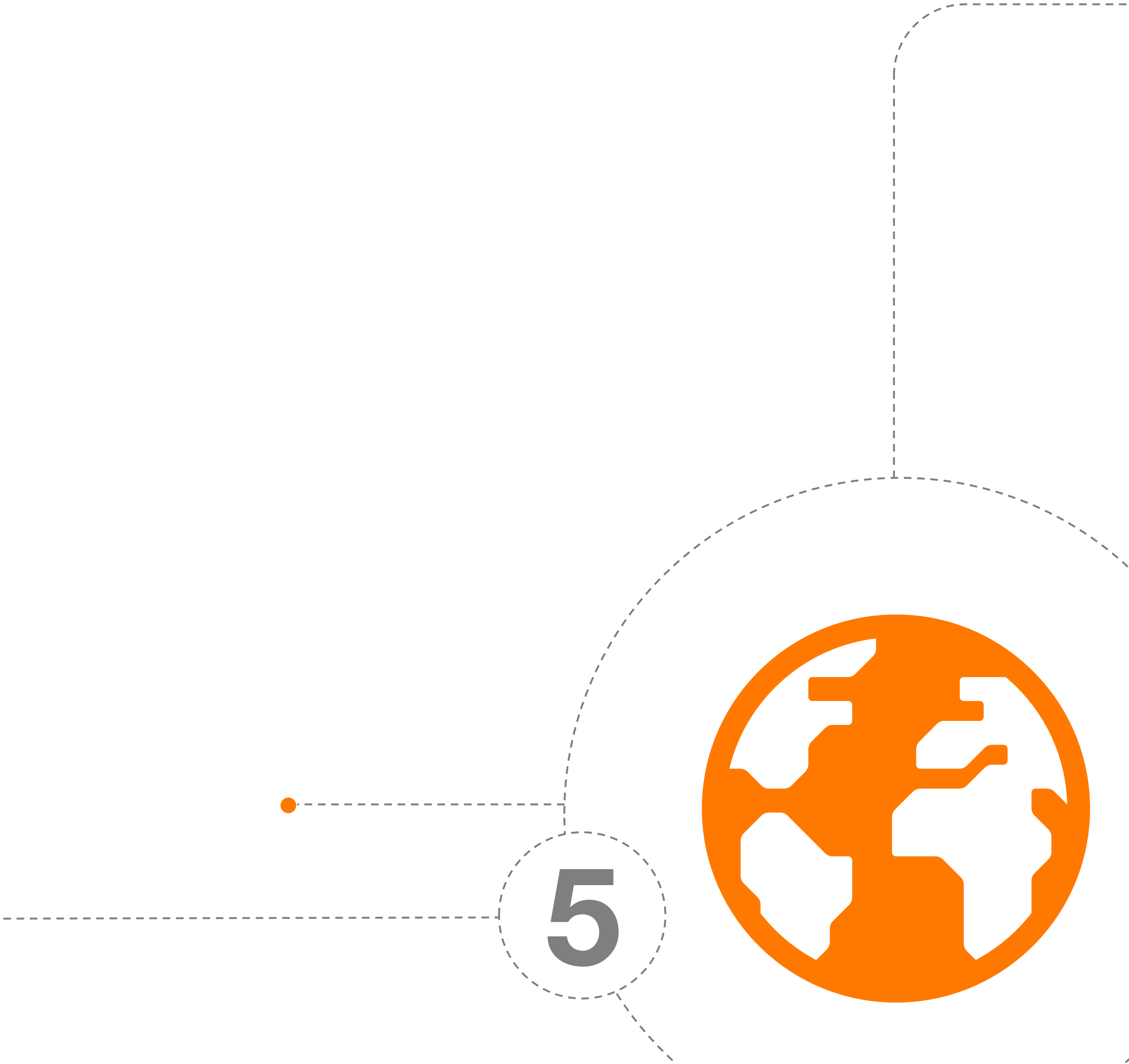
Orange
Cyberdefense

World Watch | Threat Intelligence Report

Monthly Report
May 2021



CONTENTS

CONTENTS 2

INTRODUCTION 5

OVERVIEW 6

Categories – Monthly Breakdown 7

Services Affected 9

Technologies Affected 10

Breach Trends 12

Our Recommendations 16

Cyber Extortion Trends (Beta) 20

Summary 20

General Trends 20

The number of actors is growing 21

New kids on the block 22

Best leak site. And the winner is… 22

Changes in the actor landscape 23

Victimology 25

A glance at France 29

Payment 31

Extortion Techniques 32

General Trends 33

Topic Modeling (Beta) 36

Summary 36

How we do it. 37

Good News Cyber 43

DATA BREACHES 45

Stolen ParkMobile data is now free for wannabe scammers 45

Ryuk Ransomware Attack Sprung by Frugal Student 45

Largest U.S. pipeline shuts down operations after ransomware attack 45

Ransomware attack on healthcare admin company CaptureRx exposes multiple providers across United States 45
Rapid7 source code, credentials accessed in Codecov supply-chain attack 45
Manchester City Council leaks vehicle number plate in parking ticket spreadsheet 45
Toshiba Tec France hit by DarkSide 45
Babuk ransomware group dumps D.C. Police data 45
Ireland’s Health Services hit with $20 million ransomware demand 46
23 Android apps exposed data for millions of users 46
Air India data breach impacts 4.5 million customers 46
Audio maker Bose discloses data breach after ransomware attack 46
Japanese government agencies suffer data breaches after Fujitsu hack 46
MALWARE AND EXPLOITS 47
Revealing the ‘Snip3’ Crypter, a Highly Evasive RAT Loader 47
Exploit released for wormable Windows HTTP vulnerability 47
Magecart Goes Server-Side in Latest Tactics Changeup 47
A New Watering Hole, Oldsmar and a Botnet 47
New malware campaign called WastedLoader targets unpatched IE browsers 47
XingLocker, a MountLocker variant, gets new worm capabilities 47
Microsoft: Massive malware campaign delivers fake ransomware 48
Nobelium Phishing Campaign Poses as USAID 48
VULNERABILITY MANAGEMENT 49
Microsoft Warns 25 Critical Vulnerabilities in IoT, Industrial Devices 49
Python also impacted by critical IP address validation vulnerability 49
Pulse Secure fixes VPN zero-day used to hack high-value targets 49
Apple fixes 2 iOS zero-day vulnerabilities actively used in attacks 49
Hewlett Packard Enterprise Plugs Critical Bug in Edge Platform Tool 49
Vulnerable Dell driver puts hundreds of millions of systems at risk 49
Critical 21Nails Exim bugs expose millions of servers to attacks 50
VMware fixes critical RCE bug in vRealize Business for Cloud 50
Cisco bugs allow creating admin accounts, executing commands as root 50
Qualcomm Chip Bug Opens Android Fans to Eavesdropping 50
Microsoft May 2021 Patch Update 50
Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader 50

Vulnerabilities nicknamed FRAGATTACKS affect most devices with WiFi enabled 50
May Android security updates patch 4 zero-days exploited in the wild 50
Apple fixes three macOS, tvOS zero-day bugs exploited in the wild..50
Pulse Secure VPNs Get Quick Fix for Critical RCE..50
VMware warns of critical bug affecting all vCenter Server installs 51
Asahi Linux Dev Reveals ‘M1RACLES’ Flaw in Apple M1 51
SonicWall urges customers to 'immediately' patch NSM On-Prem bug..51
HPE Fixes Critical Zero-Day in Server Management Software 51
A new weakness has been discovered in Microsoft PatchGuard..51

NOTEWORTHY 52
PortDoor Espionage Malware Takes Aim at Russian Defense Sector 52
AXA pledges to stop reimbursing ransom payments for French ransomware victims.....................................52
Train firm’s ‘worker bonus’ email is actually cybersecurity test 52
Biden issues executive order to increase U.S. cybersecurity defenses 52
DarkSide cyber extortion group bags over $9 million 52
Popular Russian hacking forum XSS bans all ransomware topics 52
ExaGrid may have paid 50 BTC thus $2.6 million in ransom to Conti gang 52
Orange Cyberdefense Presents at RSA Conference 2021 52

INTRODUCTION

Ransomware groups continue to run rampant, with one group causing quite a scene and drawing a lot of attention to themselves recently. The Colonial Pipeline, the largest fuel pipeline in the United States, had to shut down operations after suffering a ransomware attack by the DarkSide ransomware-as-a-service operators. This event was widely publicized and lead to the disruption of industries that rely on oil and fuel in that area.

In response to this, DarkSide proclaimed in a press statement that they will avoid certain targets to limit extensive impact or fall out. This also signals that the group might have underestimated or lacked appreciation of the real-life impact of their actions.

Following this, one of the most popular Russian-speaking hacker forums, XSS, banned all topics promoting ransomware. We theorize this is to prevent unwanted attention after the increased coverage of ransomware by the media and the large payments extorted from victims that created a buzz around the practice and attracted many wannabe extortionists and law enforcement agencies.

Cyber insurance and ransomware have been a hot topic since certain ransomware groups specifically target organizations that have a cyber insurance policy. In a response to this, one of Europe's biggest insurers is now suspending policies in France that reimburse victims for ransomware payments.

This month we learned of several zero-days that are being actively exploited in the wild. The affected technologies being Pulse Secure SSL VPN, iOS, macOS, tvOS, Android, and Adobe Acrobat. Fortunately, patches have been released.

VMware had a busy month, releasing security fixes for two vulnerabilities that could be exploited remotely, one of these we classified as 'Critical' severity. These affect the vRealize Business for Cloud and Virtual SAN Health Check plug-in impacting all vCenter Server deployments.

We featured a story this month that highlights the concern with the current way that Governments are handling cybersecurity. President Biden signed an executive order to modernize the US's defenses against cyberattacks and give more timely access to information necessary for law enforcement to conduct investigations. Amongst other things, it highlights that some degree of cooperation and information sharing must happen between the private and public sector.

Finally, cyber security is not all bad news! Please take a moment to **check out our new 'Good news cyber' section on page 42**, where we try to capture and reflect on some of the positive and progressive developments in our space.

At a glance

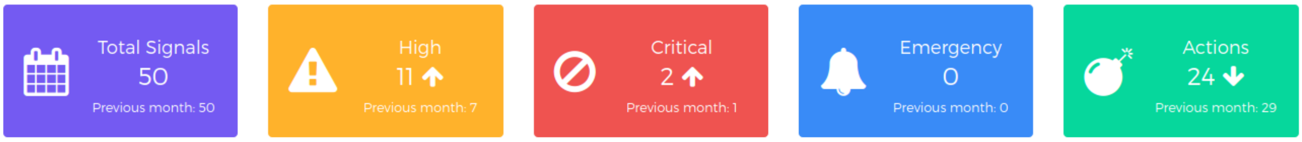
In the month of May, our researchers from the Security Research Centre, Charl van der Walt & Wicus Ross, presented their talk "All Your LAN are Belong to Us. Managing the Real Threats to Remote Workers." at RSA Conference 2021. Supporting materials, including a comprehensive solutions whitepaper, are available for you to download.

https://orangecyberdefense.com/global/rsa-2021-the-router-of-all-evil/

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	High	Critical	Emergency	Actions
50	11 ↑	2 ↑	0	24 ↓
Previous month: 50	Previous month: 7	Previous month: 1	Previous month: 0	Previous month: 29

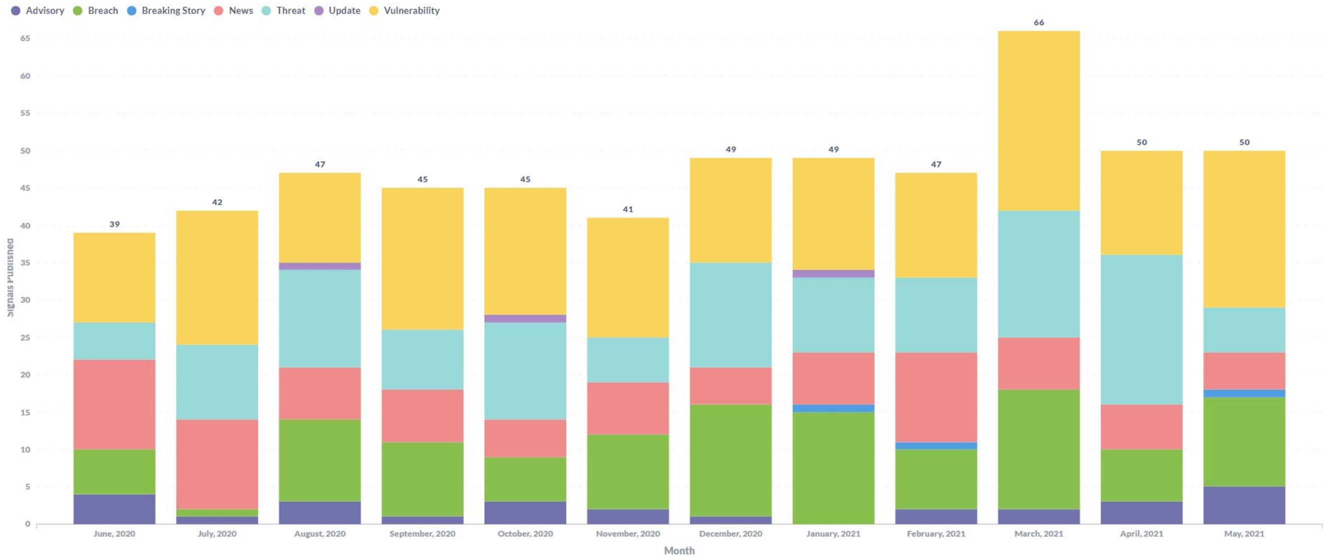
The Signal numbers for May 2021 are the same as the previous month and still higher than our rolling 12-month average of approximately 48 Signals per month. The number of actions we logged with the respective operational teams remains relatively high, but we did see a decrease from last month's record.

The number of Signals rated as 'Critical' was two and is an increase from last month. As opposed to April 2021, which had seven Signals rated as 'High' severity, May 2021 saw 11.

Our 'Signals' are organized into seven distinct categories to help you understand what kind of message we are communicating, these are:

- **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

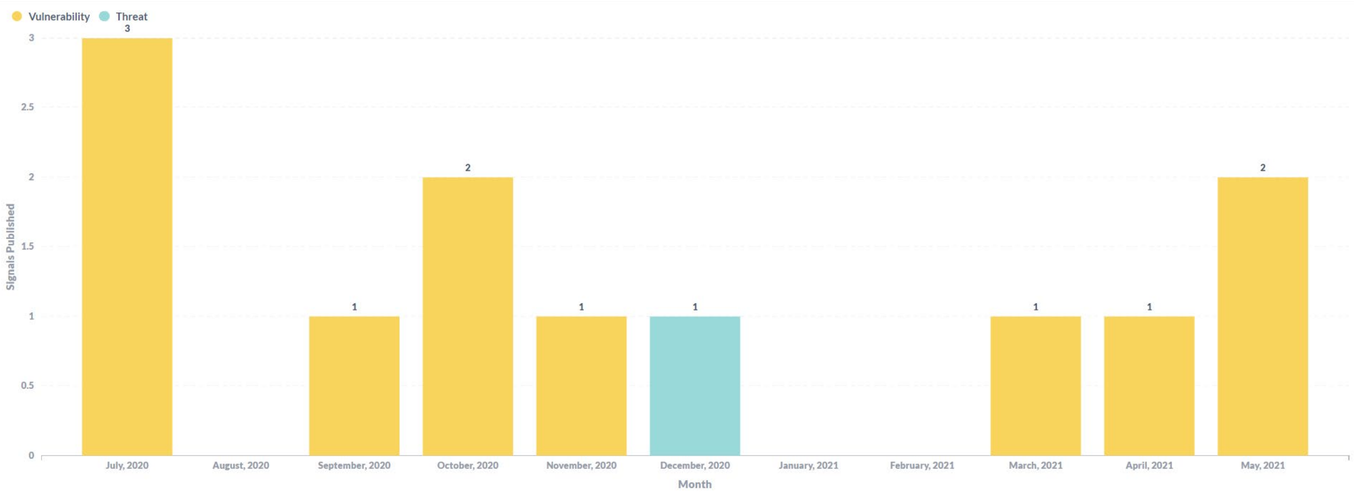


Signals by category over the last twelve months

The graph above shows the distribution of Signals across the various standard categories we track.

We published the same volume of Signals in May as in April, this month though we can see that we reported on significantly more Vulnerabilities and less Threats. Breaches are still the subject for a significant proportion of the Signals we publish, primarily these ultimately stem from cyber extortion (ransomware) attacks.

Critical Signals published over the last twelve months

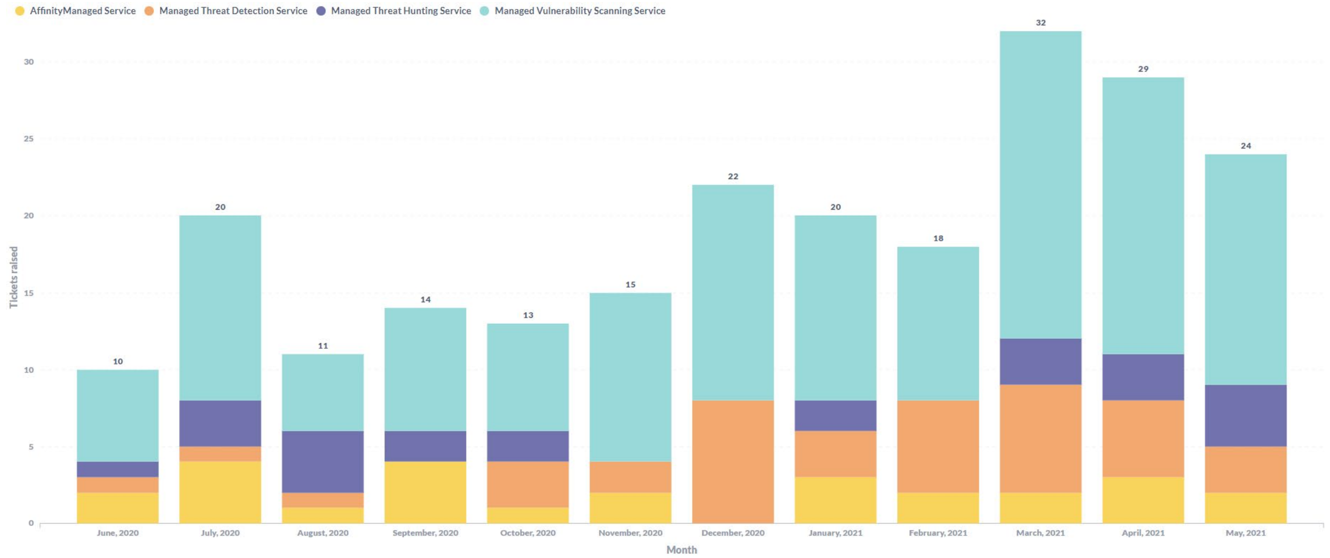


This month we published two ‘Critical’ Signals, which is quite unusual.

Herewith a list of the Critical Signals we published over the last 12 months.

Category	Date	Summary
Vulnerability	2021/05/26	VMware warns of critical bug affecting all vCenter Server installs
Vulnerability	2021/05/04	**Pulse Secure** fixes VPN zero-day used to hack high-value targets
Vulnerability	2021/04/14	**Microsoft** April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days
Vulnerability	2021/03/03	**Microsoft** fixes actively exploited Exchange zero-day bugs, patch now
Threat	2020/12/14	FireEye confirms **SolarWinds** supply chain attack
Vulnerability	2020/11/03	**Oracle** publishes rare out-of-band security update for WebLogic servers
Vulnerability	2020/10/14	Critical **SonicWall** VPN Portal Bug Allows DoS, Worming RCE
Vulnerability	2020/10/13	October Patch Tuesday: **Microsoft** Patches Critical, Wormable RCE Bug
Vulnerability	2020/09/15	Zerologon Attack Against **Windows**
Vulnerability	2020/07/15	Microsoft patches wormable SIGRed bug in **Windows** DNS Server
Vulnerability	2020/07/14	RECON bug lets hackers create admin accounts on **SAP** servers
Vulnerability	2020/07/02	**F5** TMUI Remote Code Execution Vulnerability

Services Affected



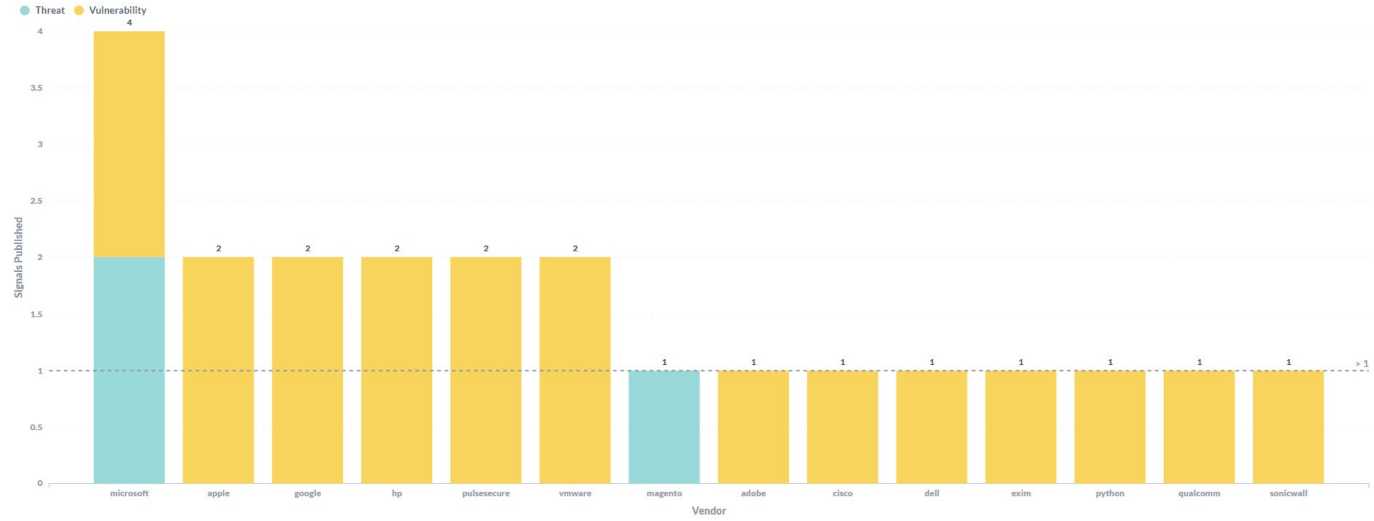
Tickets logged with our operations teams over the last 12 months

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 beginning of June 2020 is reflected on the graph above.

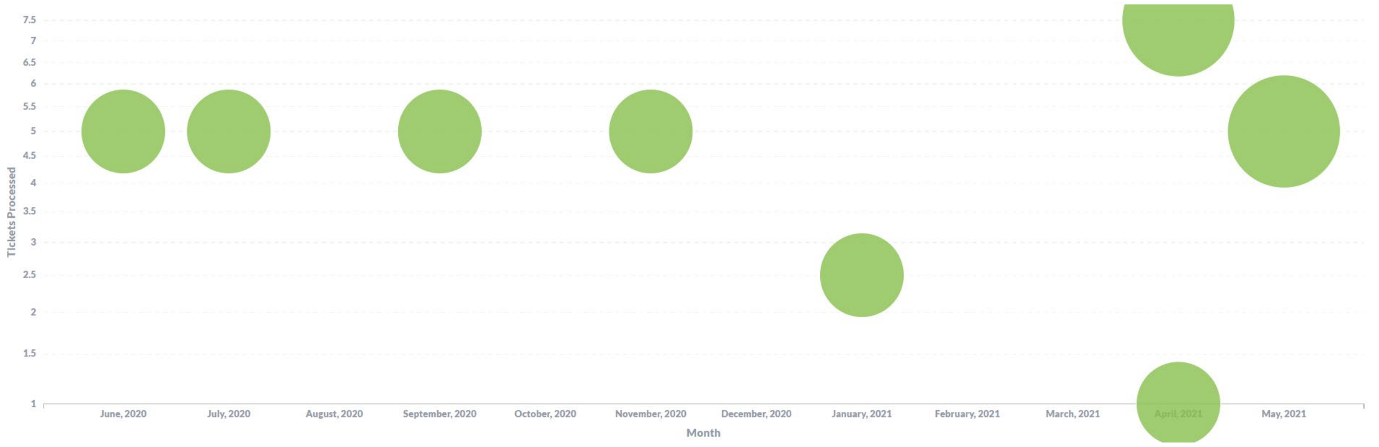
The volume of tickets raised with our Vulnerability Scanning team saw a slight drop in May but still follows the pattern of accounting for more than 50% of the tickets we raised. This is not something we expect to change anytime soon, this is borne out by the r**eports in May of zero-day vulnerabilities in Pulse Secure SSL VPN, iOS, macOS, tvOS, Android, and Adobe Acrobat** along with a critical vulnerability in VMWare vCenter Server.

Technologies Affected



Technologies featuring in our Signals in May

The chart above summarizes the technology vendors that were referenced in our Signals during May. As is to be expected, due to its popularity, Microsoft features prominently both in terms of vulnerabilities and threats. A **security technology features prominently again in May, namely Pulse Secure**, this time due to both a high and a critical severity vulnerability being disclosed.

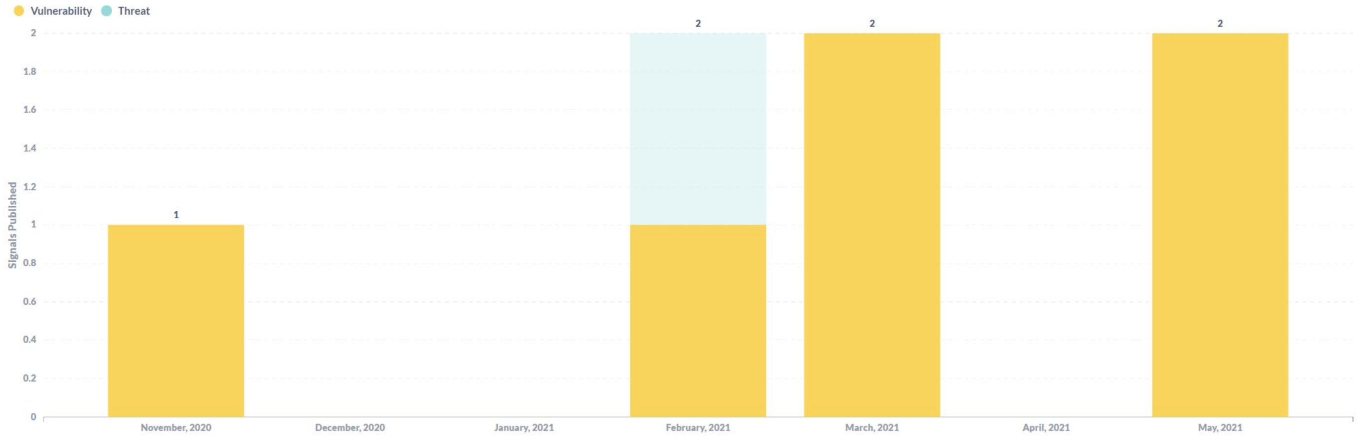


Pulse Secure vendor advisories over time

The chart above plots vulnerability advisories sent to our Security Operations by Pulse regarding their product suite. Each dot represents one or more advisories. The height on the Y axis represents the seriousness, with 10 being ‘critical’ and the size of the bubble represents the number of advisories. The chart shows clearly that **we receive a medium urgency advisory almost every month, but that there has been a slight but notable acceleration in April and May this year**. We released five advisories in those two months alone, with two serious vulnerabilities recorded in April and two medium advisories recorded in May.

Interesting also in May is the appearance of system management technologies in the form of **vulnerabilities affecting VMWare vCenter Server, HP's Edgeline Infrastructure Manager and Systems Insight Manager**. These systems can be a goldmine for attackers due to the access and control it gives them over other potentially high value systems.

We mentioned in our summary that VMWare featured significantly in our May advisories. VMware featured twice, releasing security fixes for two vulnerabilities that could be exploited remotely without credentials. One of these we classified as 'Critical' severity.



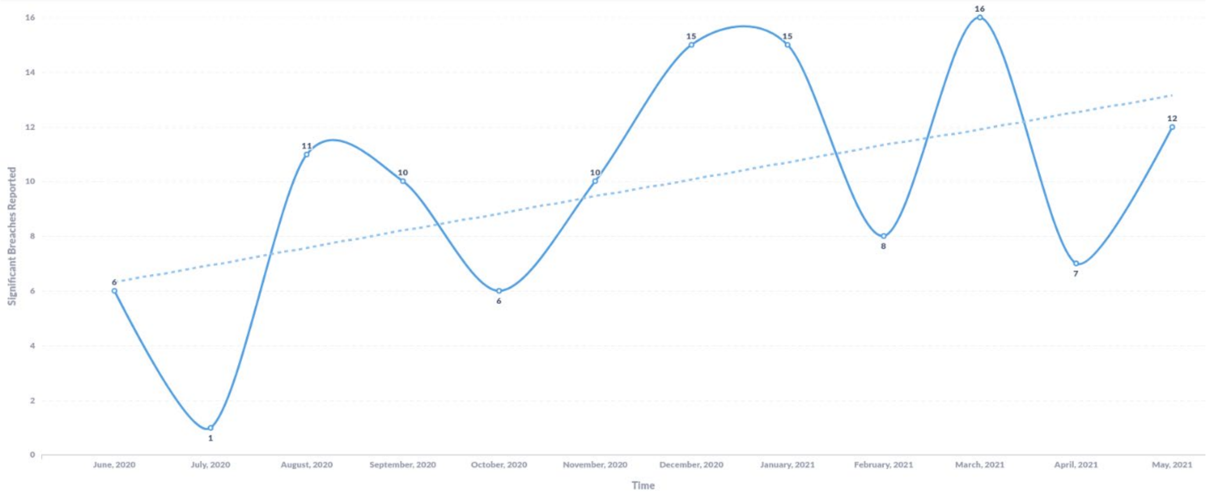
VMWare appearing in Signals over time

VMWare has only featured in 7 Signals in the last 12 months, 6 of those appearances have been in 2021 and 2 were published during May.

VMWare is particularly interesting to ransomware extortionists, since compromising the VMWare infrastructure allows operators to encrypt entire machine disk images, rather than individual files. This can significantly increase the disruptive effect and therefore the effectiveness of an attack.

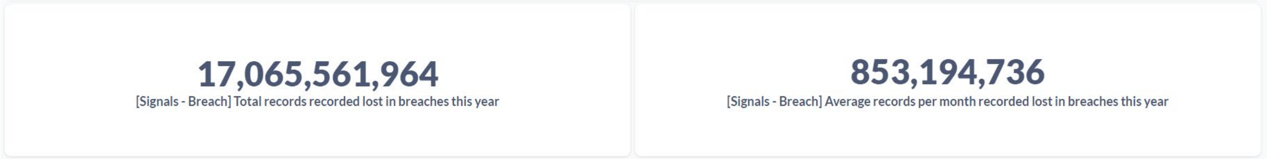
Breach Trends

As part of our research, we report on significant data breaches or compromises that we become aware of. In this section we want to explore some of the trends we are observing from the breaches we have noted and reported on.



Major breaches recorded over time

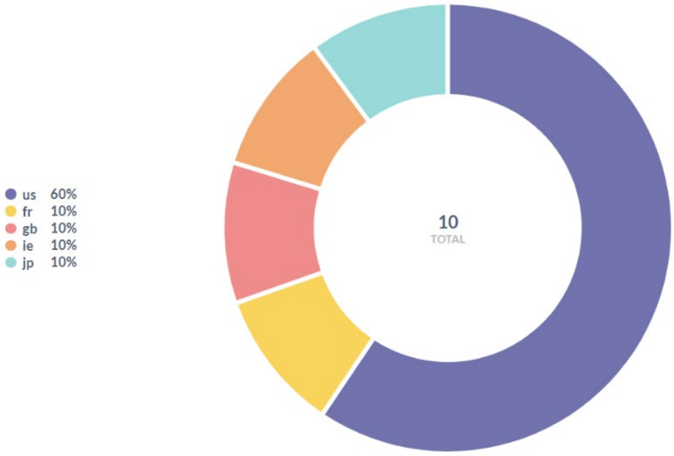
The chart above reflects the number of breaches we have reported on per month over the last 12 months.



17,065,561,964
[Signals - Breach] Total records recorded lost in breaches this year

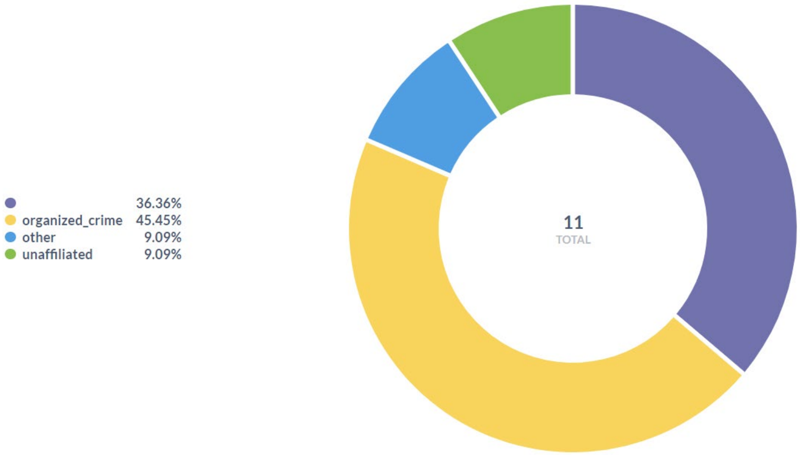
853,194,736
[Signals - Breach] Average records per month recorded lost in breaches this year

Unlike April, which seemed relatively quiet, **May saw a significant climb in the number of breaches we reported on**, with 12 Signals being categorized as a Breach. We see peaks and troughs in terms of the number of breaches reported on, however the trendline follows a clear upward trajectory and we expect that to continue.

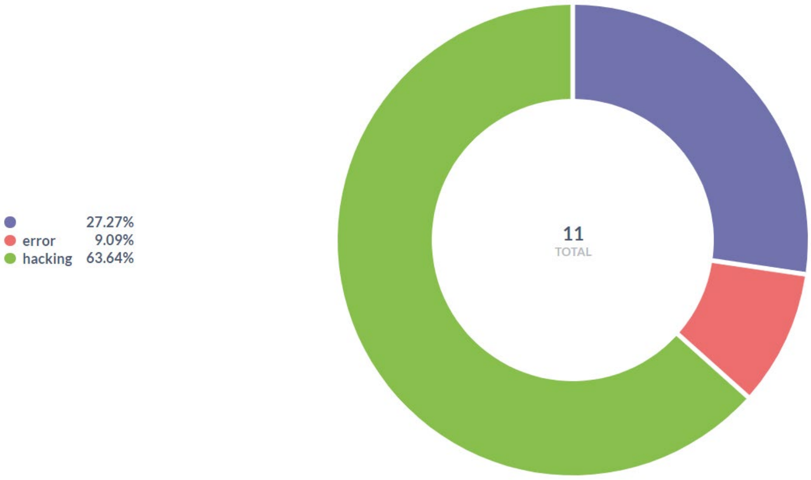


A quick review of the **12 breaches recorded in May** reveals common patterns repeating themselves:

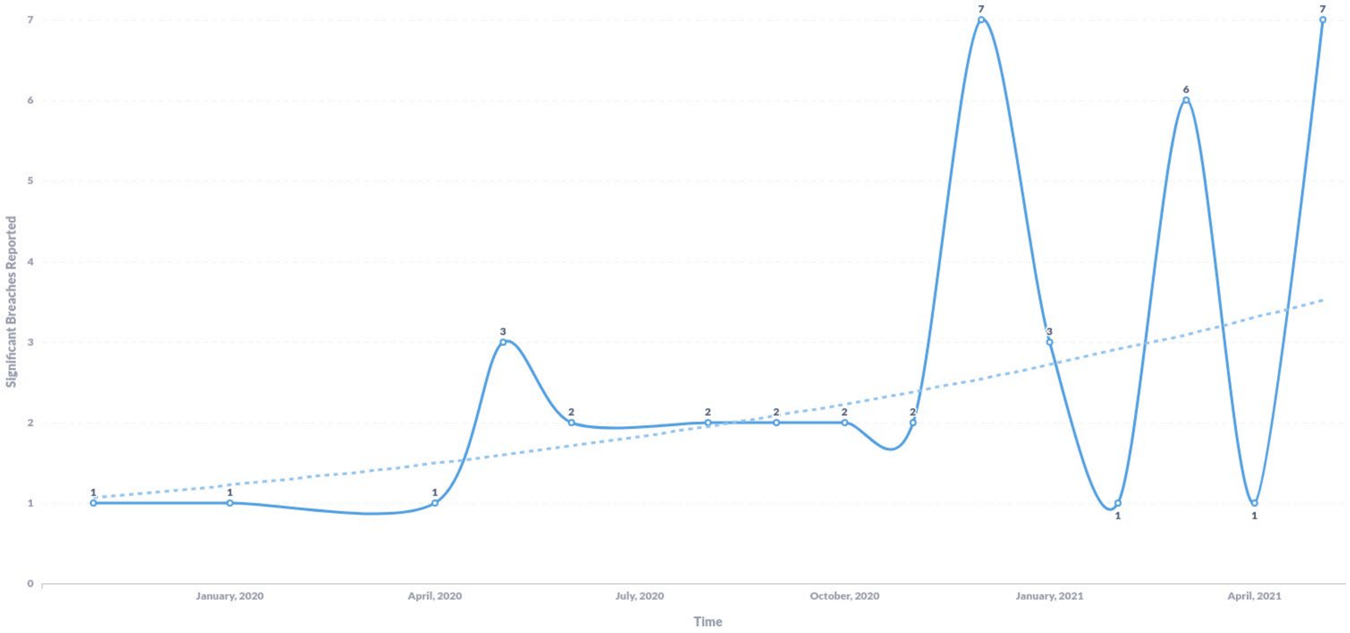
The vast **majority of reported breaches impact businesses in the USA.** From there the volumes tend to broadly track the GDP of the country. There has been **a recent increase in breaches reported out of France**, which now represents the 3rd ranked victim country, after the UK and USA. This is partly due to a spate of four breaches we recorded in France in February this year, followed by breaches in April and May.



Most publicly recorded breaches in May are attributed to organized crime groups



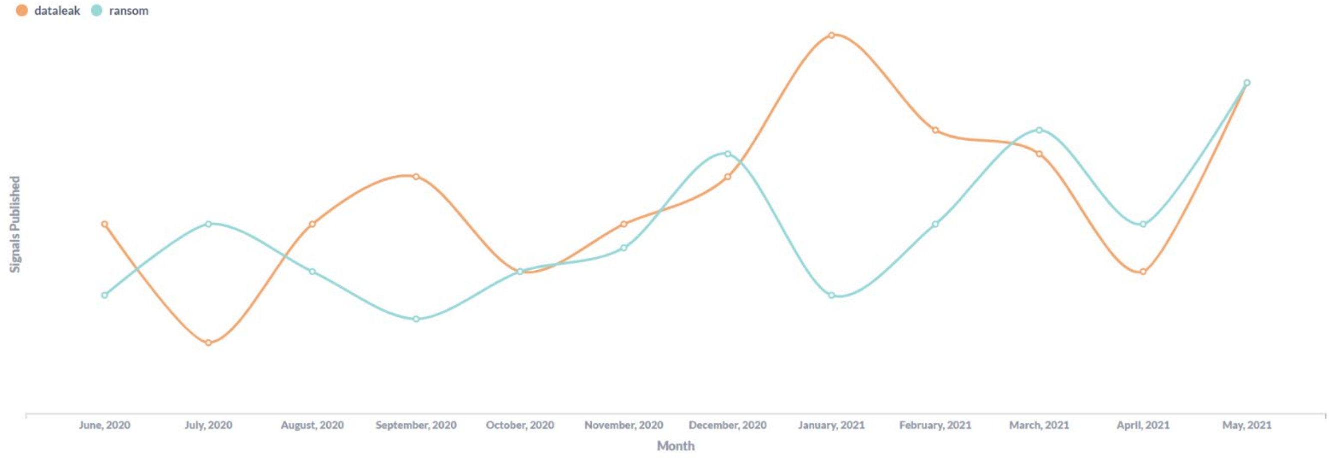
Most publicly recorded breaches in May involve 'traditional' remote hacking techniques. One breach was attributed to 'Error', only the 4th this year.



Major breaches caused by double extortion ransomware over time

Notable this month were ransomware attacks being the main cause of breaches we reported on. The trend of us reporting on double extortion ransomware related breaches can be seen in the graph below.

This correlation between 'ransomware' and data leaks can be clearly seen if we plot Signals we tag for each concept over time.



Signals tagged as dataleaks and ransomware over time

As we mentioned in the Introduction, the **Colonial Pipeline had to shut down operations after suffering a ransomware attack by DarkSide ransomware-as-a-service operators.** This event was widely publicized and lead to the disruption of industries that rely on oil and fuel in that area.

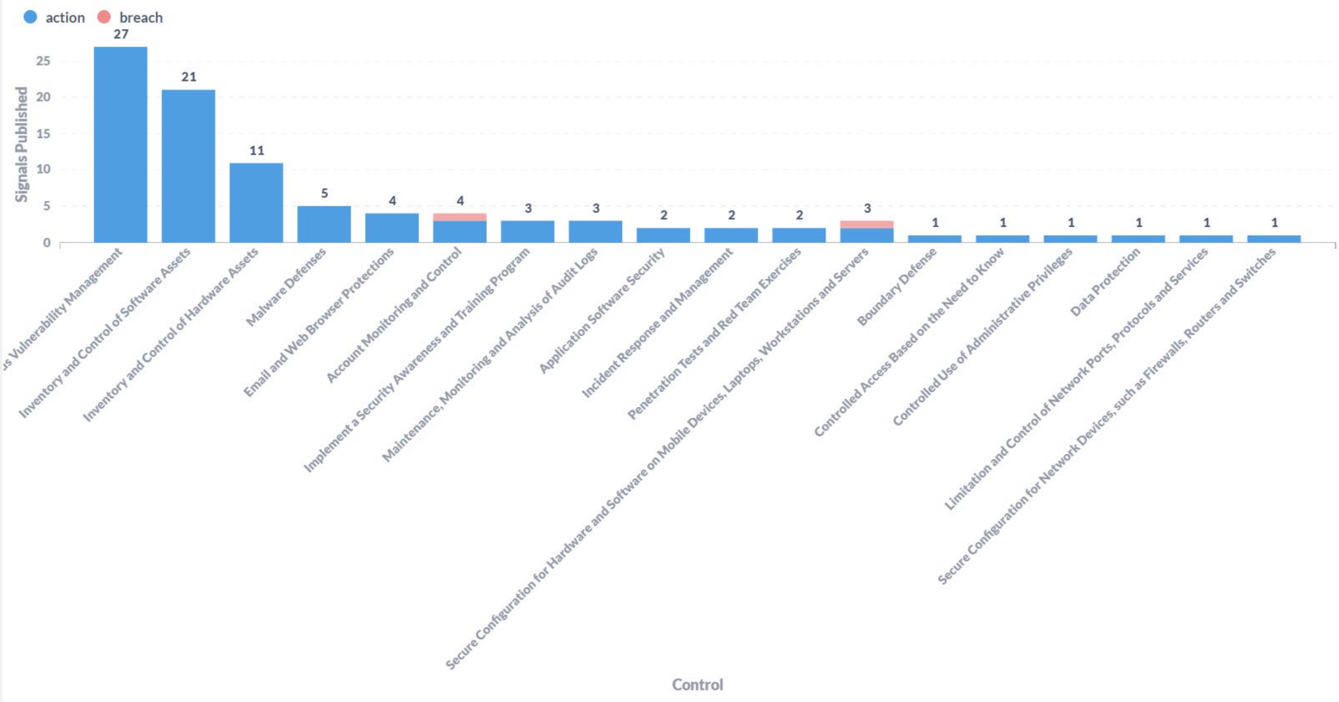
Another interesting breach was that of **a European biomolecular research institute that lost a week's worth of research data due to a Ryuk ransomware attack.** The incident was traced back to **a student who was using their own personal laptop to connect to the institute's network via Citrix.** The student wanted a personal copy of a costly data visualisation tool for their work but were unable to afford it.

Instead, they **found a “free” cracked version, that was unfortunately packed with a keylogger**. It grabbed credentials from their machine that were later used to get into the biomolecular institute.

This month we also saw how brazen some of the ransomware gangs are when **Babuk, dumped data they stole from the D.C. Police**. We know that the group published personnel files on at least 20 current and former officers after negotiations went south. The data includes home addresses, financial histories, Social Security Numbers, and results of polygraph tests. It is unclear how damaging the released information is. We know that the Babuk group claim that they have sensitive data on criminal gangs as well as data relating to Human Resources.

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

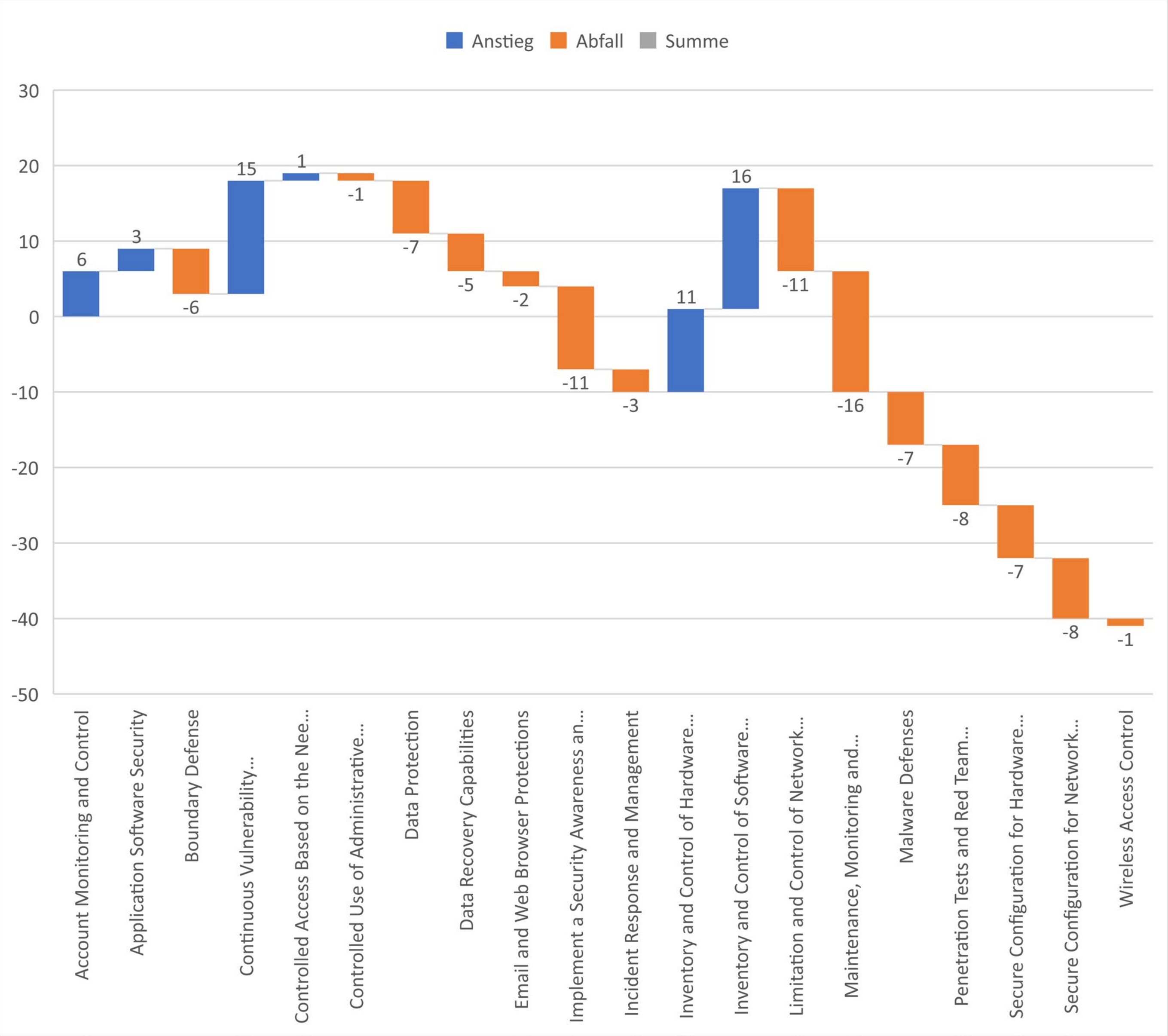


Controls linked to advisories and breaches in May

This chart summarizes the CIS controls our analysts cited in our Signals, separated between Threats and Vulnerabilities on the one hand, and the control failures we recognized 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.

It is also insightful to observe how the frequency with which these controls are cited has changed over time. The chart below compares the last five months of 2020 with the first five months of 2021:

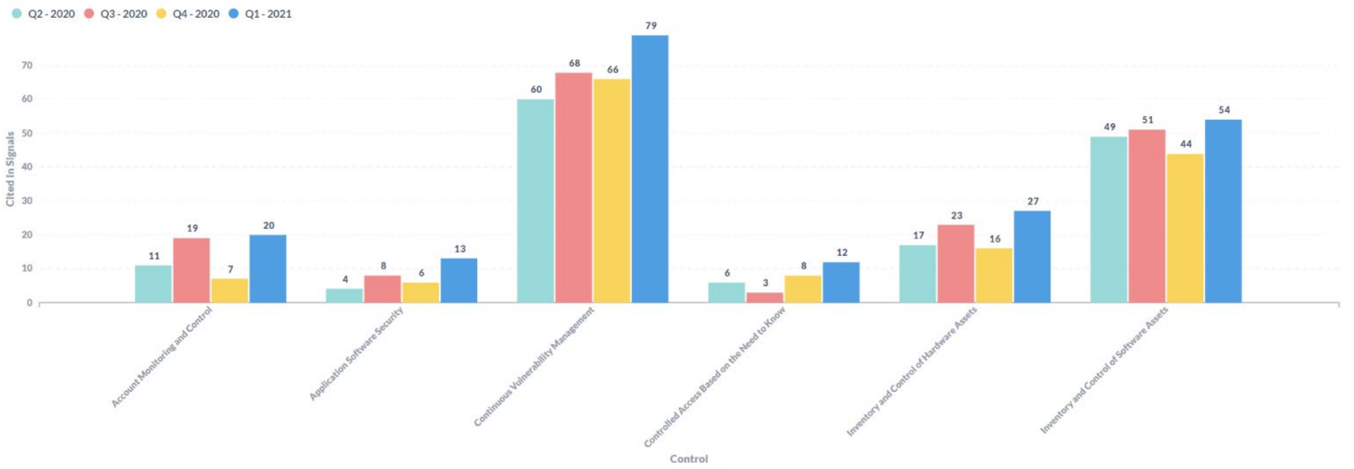


CIS security controls cited in Signals – 5 months in 2020 vs 5 months in 2021

We cited CIS security controls about 10% less since January 2021 than in the preceding 5 months. As the chart above illustrates, the big shifts percentage wise are as follows:

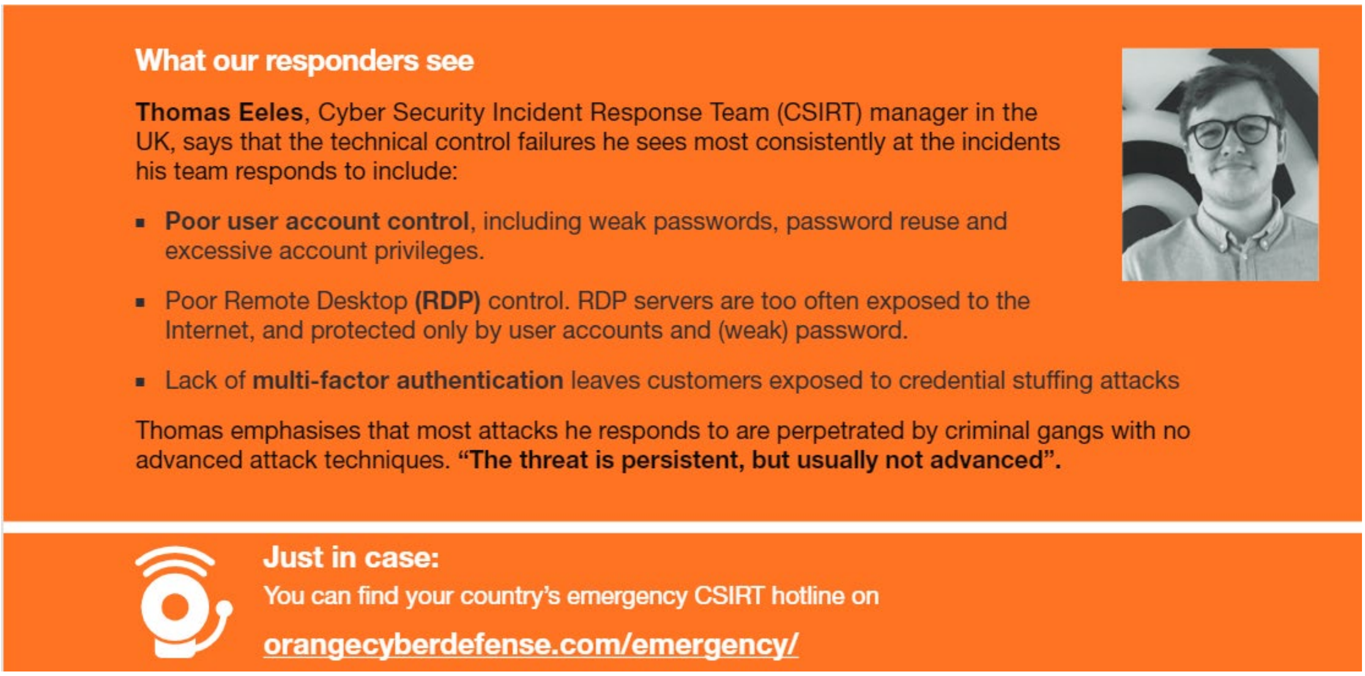
- **Account Monitoring and Control** (mentioned **55%** more often)
- **Inventory and Control of Hardware Assets** (mentioned **38%** more often)
- **Application Software Security** (mentioned **33%** more often)
- **Inventory and Control of Software Assets** (mentioned **22%** more often)
- **Controlled Access Based on the Need to Know** (mentioned **17%** more often)

We still mention Vulnerability Management and Software Inventory much more than any other controls in our advisories, but the growing prevalence of these other controls does reflect the current 'zeitgeist' and is worth noting. We have mentioned all of these controls in previous reports. The chart below tracks the prevalence of these controls in our Signals advisories for 12 months up to the end of March 2021.



CIS security controls growing more prominent in Signals

In our recent report on combatting ransomware (https://orangecyberdefense.com/global/white-papers/beating-ransomware/) we shared the following insight from our Computer Security Incident Response (CSIRT) team:



What our responders see

Thomas Eeles, Cyber Security Incident Response Team (CSIRT) manager in the UK, says that the technical control failures he sees most consistently at the incidents his team responds to include:

- **Poor user account control**, including weak passwords, password reuse and excessive account privileges.
- Poor Remote Desktop **(RDP)** control. RDP servers are too often exposed to the Internet, and protected only by user accounts and (weak) password.
- Lack of **multi-factor authentication** leaves customers exposed to credential stuffing attacks

Thomas emphasises that most attacks he responds to are perpetrated by criminal gangs with no advanced attack techniques. **"The threat is persistent, but usually not advanced".**

Just in case:
You can find your country's emergency CSIRT hotline on
orangecyberdefense.com/emergency/

In the same paper we make the argument that the basics in defeating extortion attacks primarily involve the principle of **least privilege** and network **segmentation**.

However, we go on to describe **a set of low-hanging controls, that can be implemented to combat the threat of ransomware and extortion attacks**:

1. **Secure VPNs and firewalls.** Many attacks target vulnerabilities in perimeter security technologies. Make you sure you patch them, configure them properly and ensure unique, strong, passwords.

2. **Secure Remote Desktop.** Like perimeter security, remote access is proving to be too rich a target. Take it off the internet, put it behind your VPN, patch and configure it properly, and ensure passwords are strong and unique.

3. **Educate your users.** Employees can be the weakest or strongest link in your security chain. Make sure you equip and motivate them to make good security decisions.

4. **Use a password vault.** Vaults support the use of strong and unique passwords for all systems. It is critical that your administrators are using one, but we would advocate for sponsoring a password vault application for all your employees, even to use for their private accounts.

5. **Upgrade SMB.** Many lateral movement techniques in Microsoft Active Directory environments leverage inherent weakness in the Server Message Block (SMB) protocol. If at all possible, you should disable SMBv1 across your entire estate and upgrade to v3 (or v2 if necessary).

6. **Optimize your EDR.** Make sure you have a good solution that is properly deployed and well managed.

Cyber Extortion Trends (Beta)

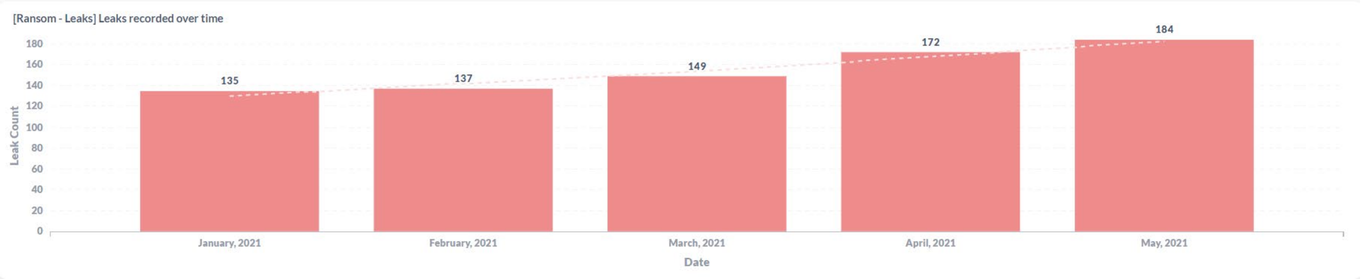
Summary

We noted the following high-level developments during our research in May:

- We have recorded 777 new extortion leaks between the beginning of January and the end of May this year. These are only from the sites that we know about and are able to monitor.
- Total number of leaks we have been able to observe has **grown by about 7% in May.**
- The total number of actors in our database has increased to 28, with 21 distinct groups considered active in May.
- We note the emergence of several groups that we have observed using leak sites for the first time in May, including ArvinClub, AstroTeam, Grieflist, LV2 & Prometheus.
- After an almost meteoric rise, just as we were completing this report, the **Avaddon group announced its 'retirement'** and shared 2,934 decryption keys for victims with the media outlet Bleeping Computer.
- DarkSide, the group responsible for the Colonial Pipeline attack, had been increasing their activity slowly until they lost control of their infrastructure and went offline after mid-May.
- The **biggest increase in victims was in Education**, which recorded 7 more victims in May than in April. However, most observed **extortion demands remain concentrated in the Manufacturing and Professional Services industries.**
- Despite the popular use of the term 'Big Game Hunting', and the attention paid by the media to big-name attacks, **most of the victims we observe are categorized as 'Small' businesses.**
- Several compromises occurred again in Italy, while in France the dip in April was reversed and the country recorded its second highest number of observed leaks. **France, the UK, and other European powers have been trending upward over time, while volumes in the US and Canada have decreased**, so that **France now ties with Canada** as the second most common geography for victims.

General Trends

Through our ransomware leak site monitoring program, we have succeeded in documenting a set of **777 ransomware leaks since January**. We do not yet have sufficient data in through this program to seriously comment on trends over time, but we are able to present some insights based on the data we have.

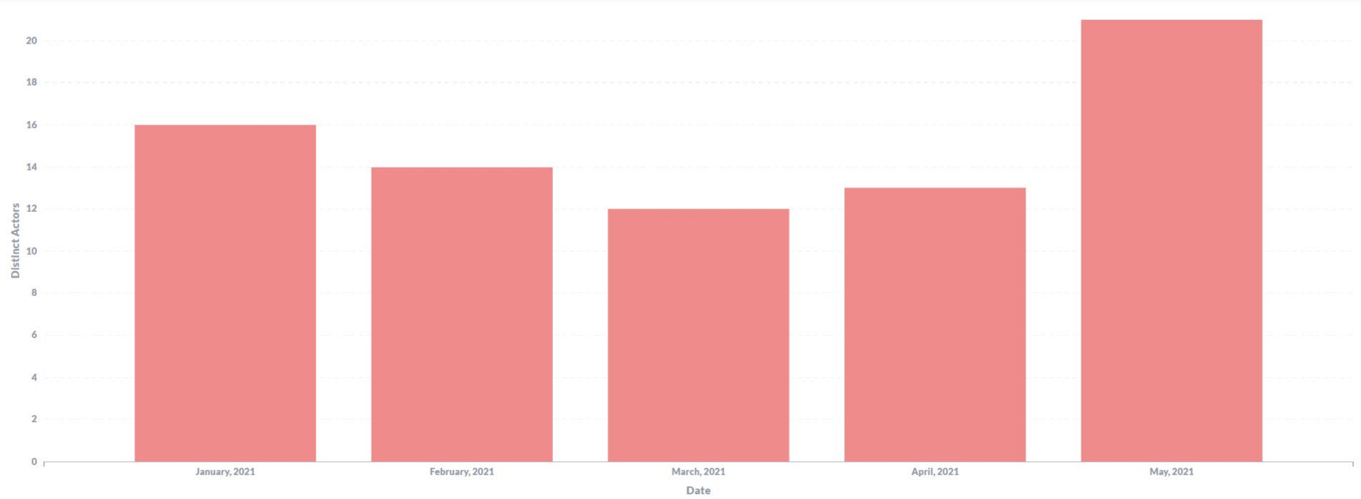


Total leaks observed over time – YTD 2021

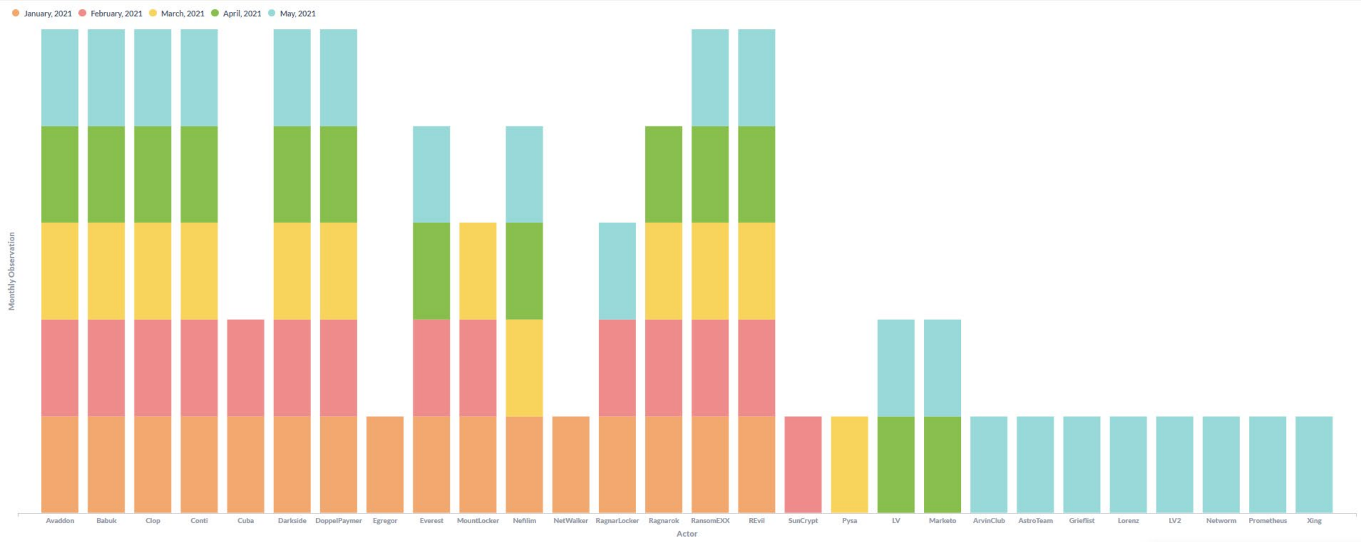
The total number of leaks we have been able to observe has **grown by about 7% in May over April**.

The number of actors is growing

The total number of actors in our database has increased to 28. In addition, the number of actors leaking to sites we can observe increased substantially from 13 in April to 21 in May:



Distinct number of observed Threat Actors over time – YTD 2021



Distribution of distinct actors observed per month – YTD 2021

As the chart above illustrates, several actors have been persistently active since the beginning of the year, including Avaddon, Babuk, Cl0p, Conti, DarkSide and others. Other actors like Egregor and Netwalker were observed only at the beginning of the year, but not again since. Both these groupings were disrupted by law enforcement activities leading to arrests of either the core developers or the affiliates.

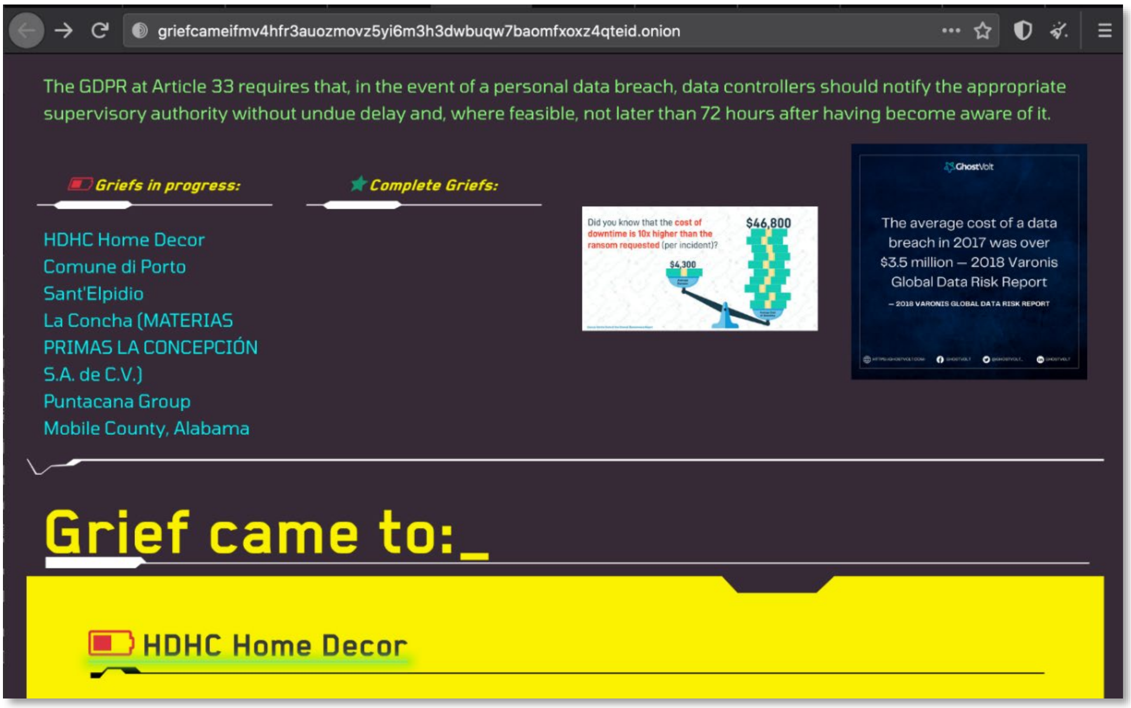
Other groups have almost certainly rebranded or been amalgamated. A good example of rebranding is Babuk, who has kept their onion address of their leak site but has rebranded to the name ‘Payload.bin’ and introduced a new look and feel for their leaksite on the dark web. The rebrand happened at the end of May and is therefore not yet reflected in our data.

New kids on the block

We also note the emergence of several groups that we're observed using leak sites for the first time in May, including ArvinClub, AstroTeam, Grieflist, LV2, Prometheus, and others.

1. **Prometheus** refers to itself as a "Group of REvil", which means REvil is connected to 2 other groups. "LV blog" being the other.
2. "**Grief list**" - Grief or Pay is a new player with a very impressive page, which is entertaining and "informative". See the example below
3. "**Arvin Club**" is not actually a new player, but we have not been able to track them before now. They are more of a marketplace similar to Marketo, selling data leaks that don't necessarily involve data encryption and thus a ransomware attack. The data leaks could potentially also originate from other attack types than ransomware.
4. "**File leaks**" renamed to "**SynACK / File Leaks**". However, we have not been tracking them to date.

Best leak site. And the winner is…


griefcameifmv4hfr3auozmovz5yi6m3h3dwbuqw7baomfxoxz4qteid.onion

The GDPR at Article 33 requires that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Griefs in progress:

HDHC Home Decor
Comune di Porto Sant'Elpidio
La Concha (MATERIAS PRIMAS LA CONCEPCIÓN S.A. de C.V.)
Puntacana Group
Mobile County, Alabama

Complete Griefs:

Did you know that the cost of downtime is 10x higher than the ransom requested (per incident)?

$4,300 $46,800

GhostVolt

The average cost of a data breach in 2017 was over $3.5 million – 2018 Varonis Global Data Risk Report

– 2018 VARONIS GLOBAL DATA RISK REPORT

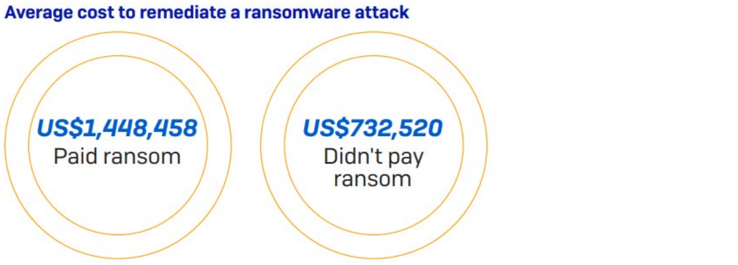
Grief came to:_

HDHC Home Decor

Grief List wins the new extortion leak site of the month award

The Grief List site, featured above, has all the attributes of a 'good' modern leak site, but ups the ante even further by citing diverse reports and statistics apparently in support of the payment of ransoms.

Interesting to note is Grief's assertion that the 'cost of downtime is higher than the ransom requested per incident'. Our perspective is unsurprisingly different. Apart from the cumulative downside impact that payment has by fueling the cybercrime ecosystem, a recent survey by Sophos reveals[1] that **paying the ransom doubles the cost of dealing with a ransomware attack.** Companies that pay the ransom still generally also have to invest in professional services and more to support their recovery from the event.

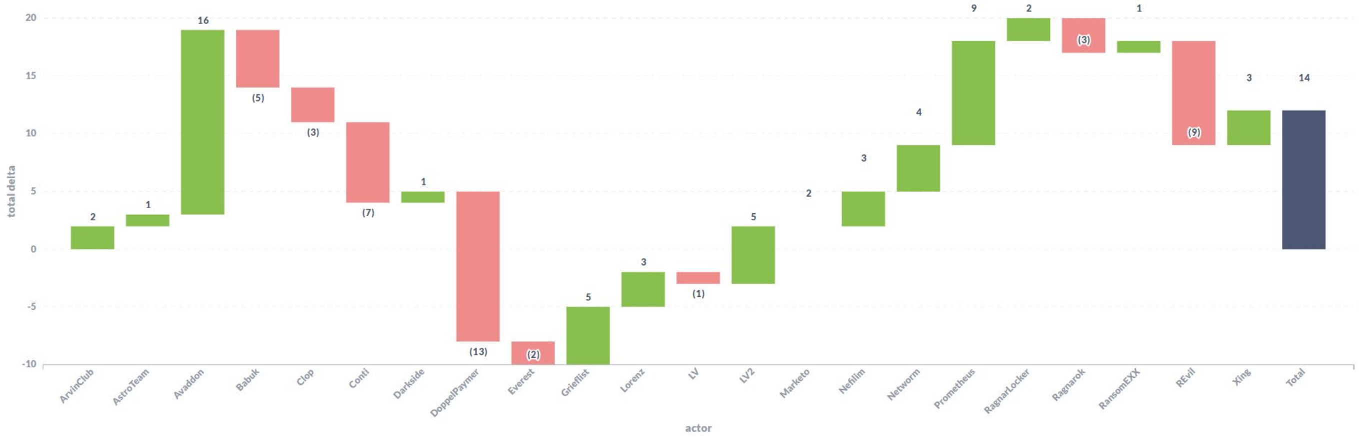


Did your organization get the data back in the most significant ransomware attack? Data only represents respondents whose organization's data had been encrypted in the most recent ransomware attack. Base: 1,849 respondents. **Paid the ransom** combines responses "Yes, we paid the ransom" and "No, even though we paid the ransom." **Didn't pay the ransom** combines responses "Yes, we used backups to restore the data," "Yes, we used other means to get our data back," and "No, we didn't pay the ransom."

Sophos reports that it is much more expensive to pay the ransom

Changes in the actor landscape

Among the various ransomware crews the level of activity has varied substantially, as the chart below reveals.

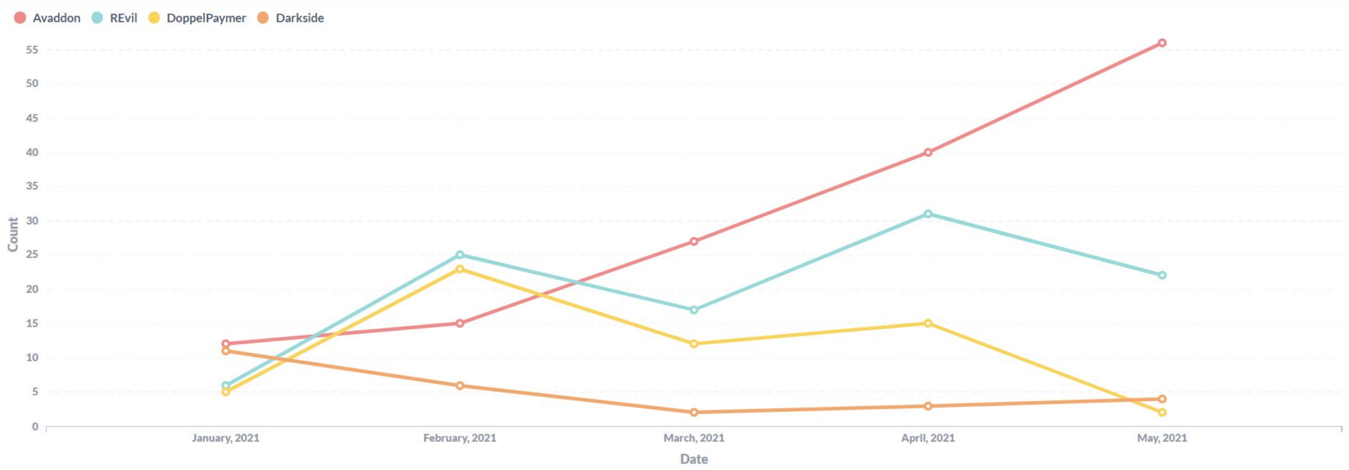


Double Extortion actors – changes since April

The shifts have obviously been with Avaddon (up), Doppelpaymer (down) and REvil (down). DarkSide, despite the 'heat' they experienced from the Colonial attack, still managed to clock one more leak than in the previous month.

We examine the performance of these actors over time.

- [1] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

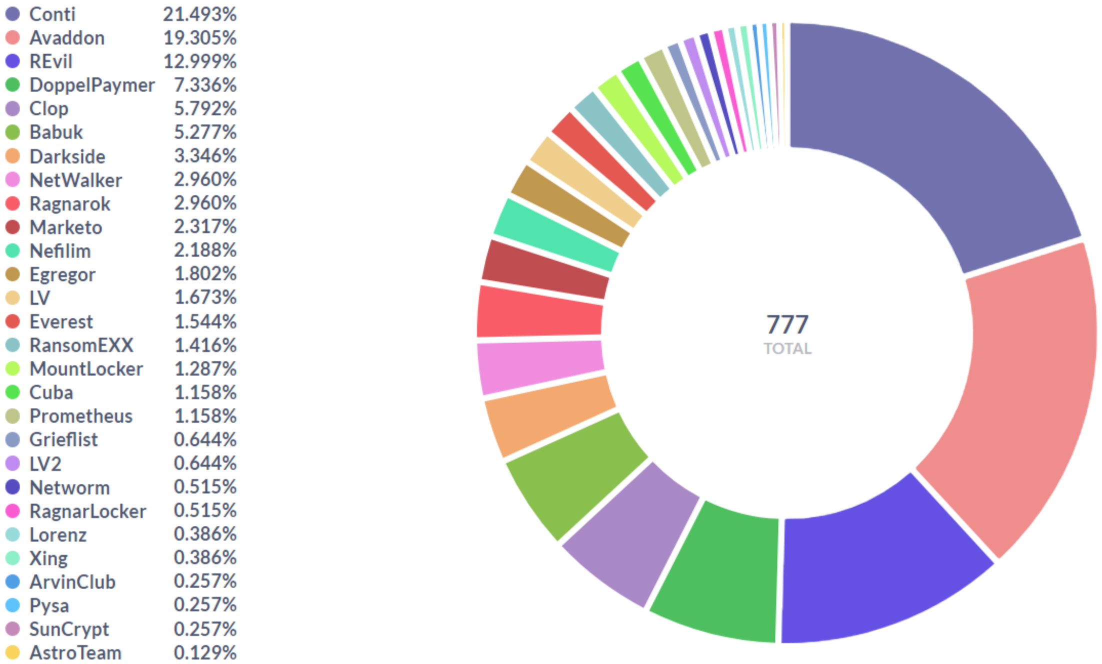


Avaddon, Doppelpaymer, REvil, and. DarkSide over time

The chart above clearly shows the **meteoric increase in activity by Avaddon**. REvil did lower volumes in May compared to April but is still growing in activity overall. Doppelpaymer appears to be on a slight downward trajectory.

DarkSide activity had been increasing slowly until they lost control of their infrastructure and went offline after mid-May. Despite (or perhaps because of) their recent notoriety they remain a small player in the grander scheme of things.

The net effect of these new leaks reveals the relative position of the 28 players we're monitoring as follows:



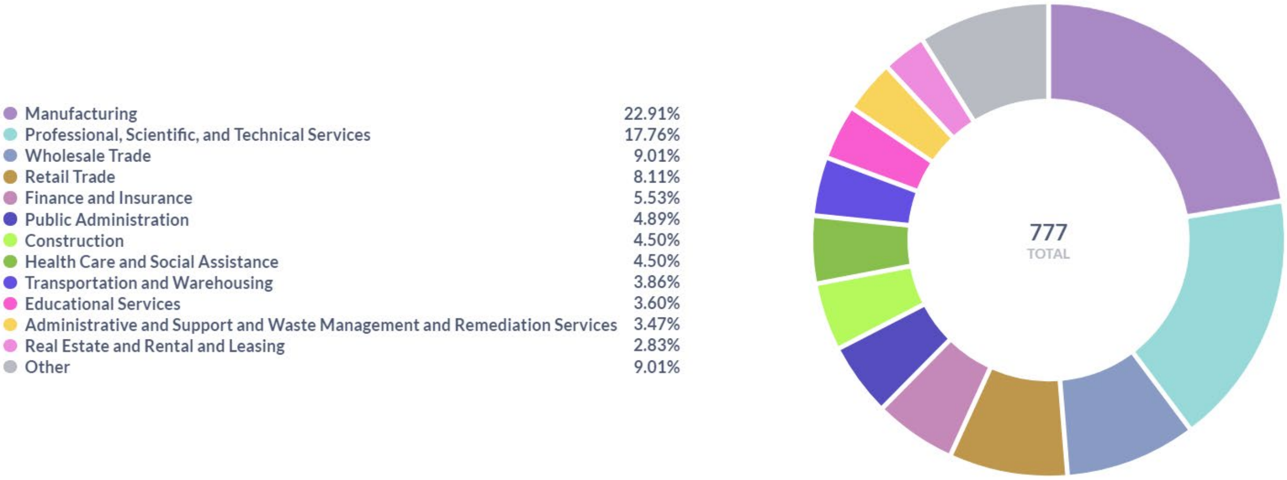
Ransomware leaks by Actor – YTD 2021

In a surprise development, just as we were completing this report, the **Avaddon group announced its ‘retirement’ and in fact shared 2,934 decryption keys for victims with the media outlet Bleeping Computer**[2]. As we have noted previously, Avaddon has been steadily increasing the scale of its operations and as of the end of May was considered to be the second most active operator, just after Conti.

It is not clear yet what prompted this move by Avaddon, or what its future impact will be, but **it is reasonable to assume that their skills and resources will emerge in some other form elsewhere in the ecosystem.** We will continue to monitor this development in future reports.

Victimology

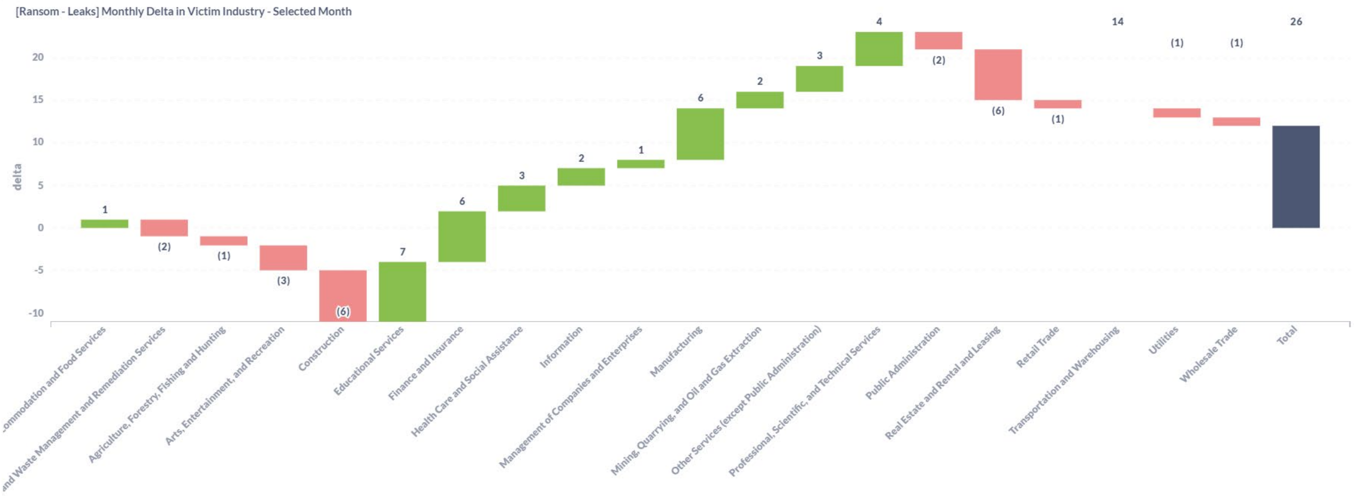
The familiar patterns in victimology persist.



Extortion victims by Industry – YTD 2021

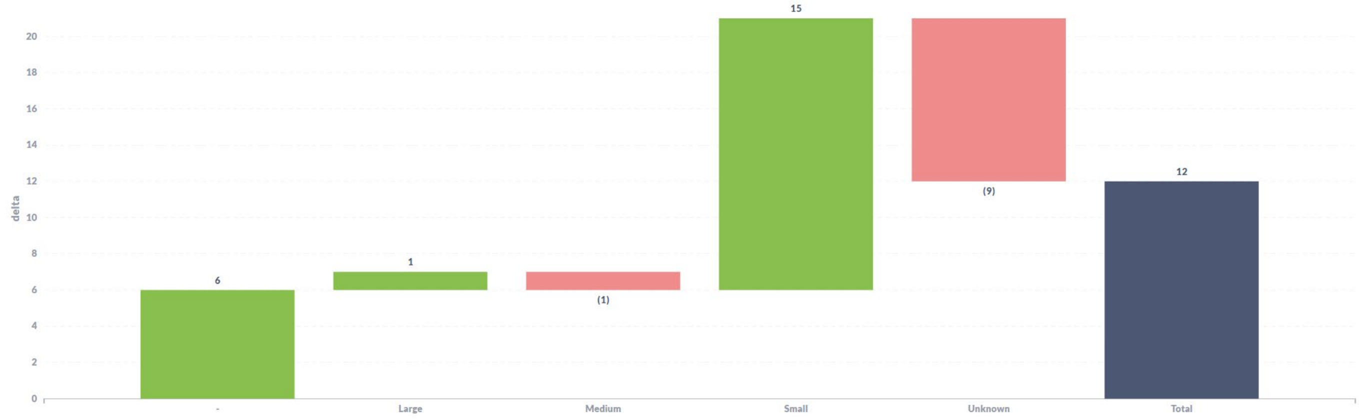
We note that most observed **extortion demands remain concentrated in the Manufacturing and Professional Services industries.** As we have argued before, however, **it would be a mistake to assume this puts other industries less at risk.** These victims only become visible to us once the entire attack has succeeded and their data is already stolen and encrypted. **We believe the victim demographics have as much to do with the vulnerability of the victims as the preferences of the criminals.**

[2] https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/



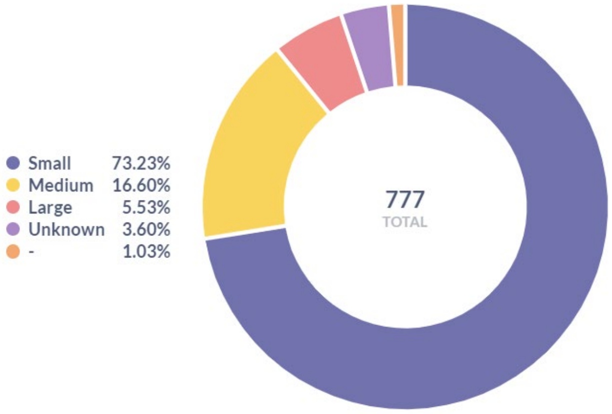
Changes in victim industry counts from April to May

As we can see from the waterfall chart above, there were indeed several new victims observed in the Manufacturing and Professional Services industries, but **the biggest increase in victims was in Education**, which recorded 7 more victims in May than in April. Victims in the education space still only represent less than 4% of our total 2021 database.



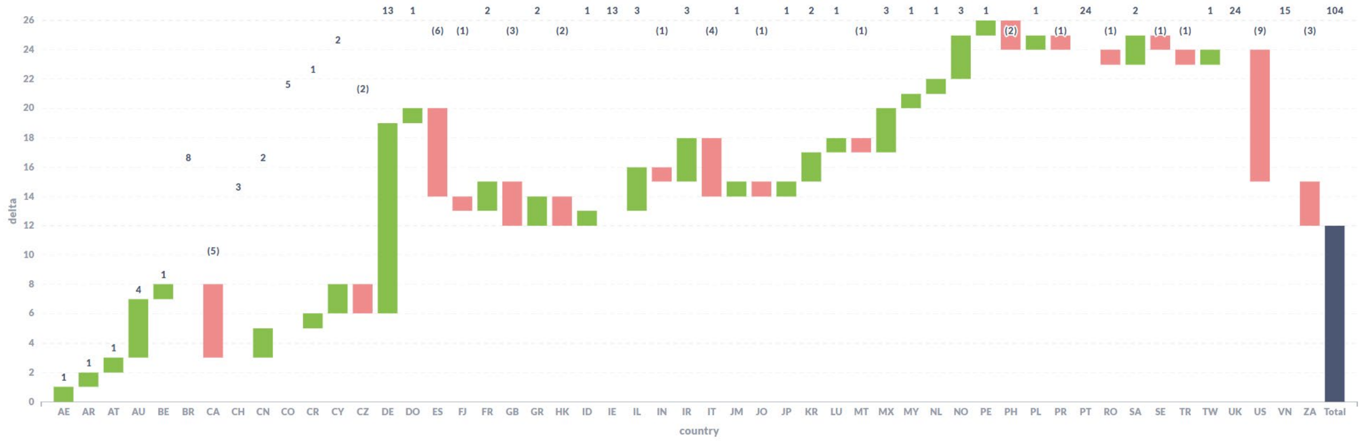
Changes in victim size counts from April to May

In May we also see familiar patterns repeated with respect to the size of the victims. Despite the popular use of the term ‘Big Game Hunting’, and the attention paid by the media to big-name attacks, **most of the victims we observe are categorized as ‘Small’ businesses.** Large businesses, likely with more resources, skills and technology at their disposal, are significantly less likely to end up on a leak site.



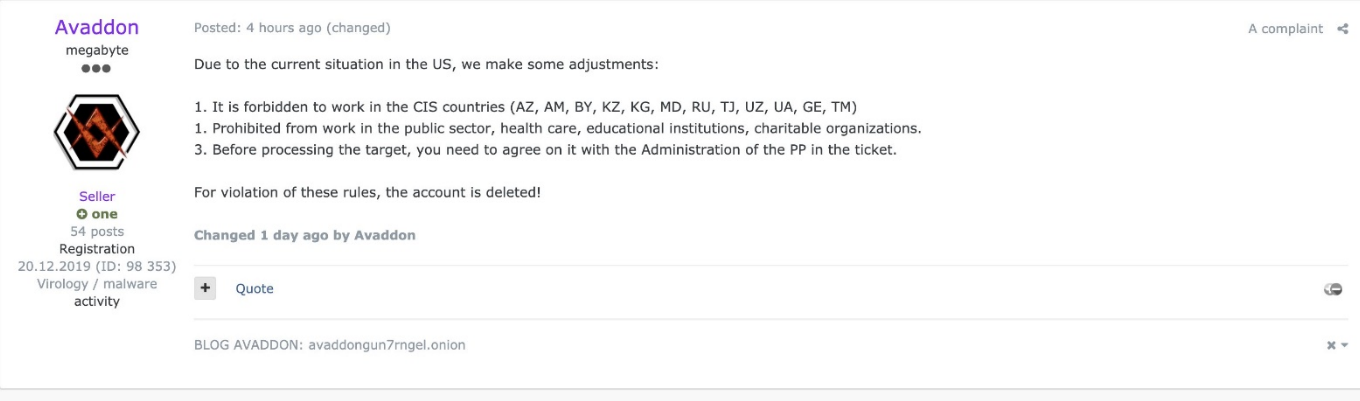
Observed Victims by Size – YTD 2021

In a sense this trend may be viewed in a positive light. Despite the potentially higher rewards that may be gleaned from compromising large business, attackers appear to favour smaller, weaker, targets, suggesting that **the appropriate deployment of contemporary security controls can have a deterrent effect.**



Changes in victim Country from April to May

A review of the leak victim's geographical presence reveals a decrease in US victims from April to May, with a corresponding increase in victims from Germany. There may be reason to believe that the recent increase in attention given to 'ransomware' in the US after the Colonial Pipeline attack has encouraged criminals to seek victims elsewhere, but it is too soon to say that with certainty.



Posted: 4 hours ago (changed)

Due to the current situation in the US, we make some adjustments:

1. It is forbidden to work in the CIS countries (AZ, AM, BY, KZ, KG, MD, RU, TJ, UZ, UA, GE, TM)
1. Prohibited from work in the public sector, health care, educational institutions, charitable organizations.
3. Before processing the target, you need to agree on it with the Administration of the PP in the ticket.

For violation of these rules, the account is deleted!

Changed 1 day ago by Avaddon

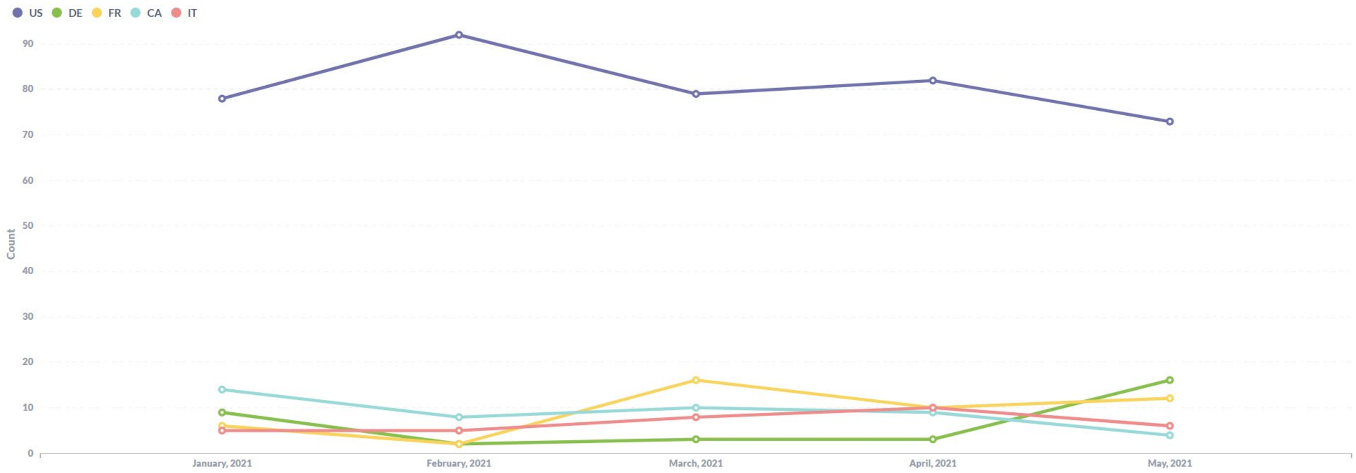
BLOG AVADDON: avaddongun7rngel.onion

https://twitter.com/John_Fokker/status/1393225076846301186/photo/2

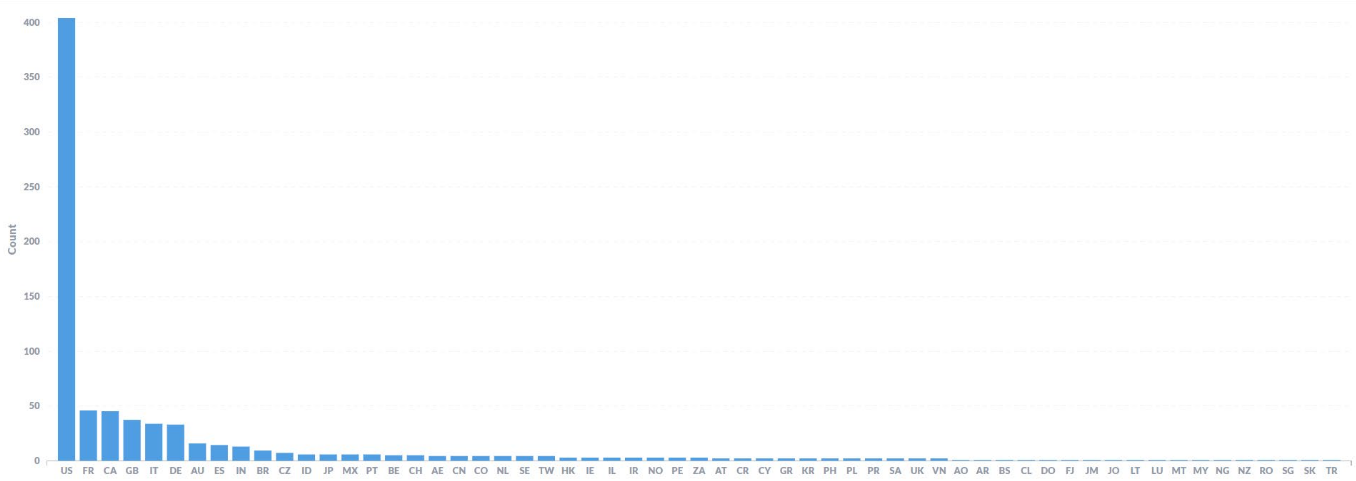
A glance at France

In our March report we noted volumes of incidents impacting Italian and French businesses. In France we had observed a massive spike in compromises during March, but in April the number of French victims dropped again. In Italy, however, the number of monthly victims increased slightly in April.

We review these trends again this month, noting that several compromises occurred again in Italy, while **in France the dip in April was reversed and the country recorded its second highest number of observed leaks** since we started tracking.



Ransomware leaks in France and Europe continue to trend upward while the US and CA decrease

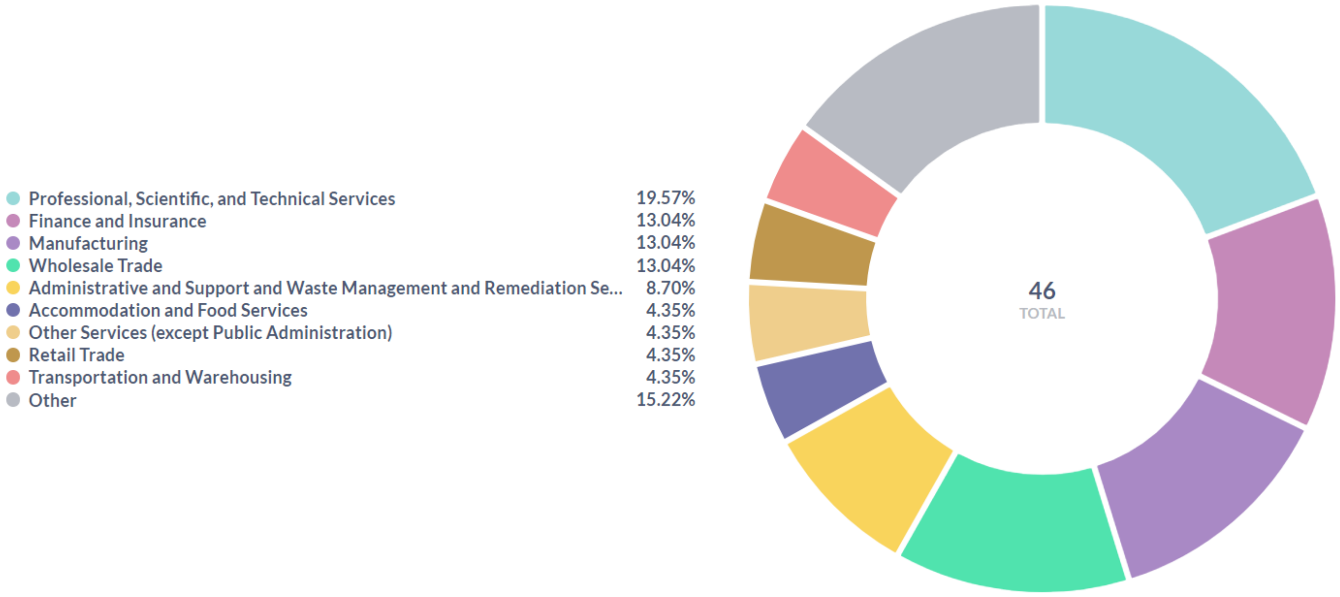


France and Canada now the second most common victim countries

As we can note from the chart above, **France now ties with Canada as the second most common geography for victims. With a surge in May, Germany now assumes 4th place.**

In general **victim geography counts appear to correlate broadly with the size of the country's economy,** yet there can be no doubt that **France, the UK, and other European powers have been trending upward over time, while volumes in the US and Canada have decreased.** Assuming this trajectory continues, countries like France, Italy, Germany and the UK will soon surpass Canada in leak victim volumes.

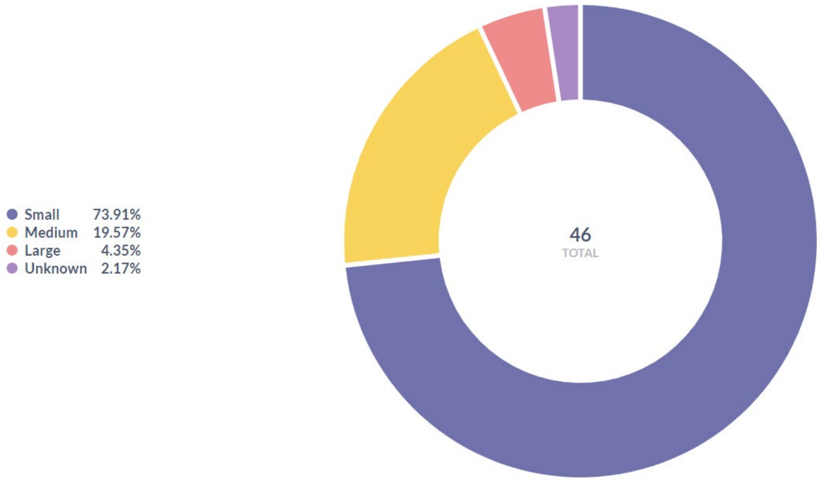
Given the concentration of our operations in France, we pause to examine victim demographics in that country.



Distribution of Industries across French leak victims

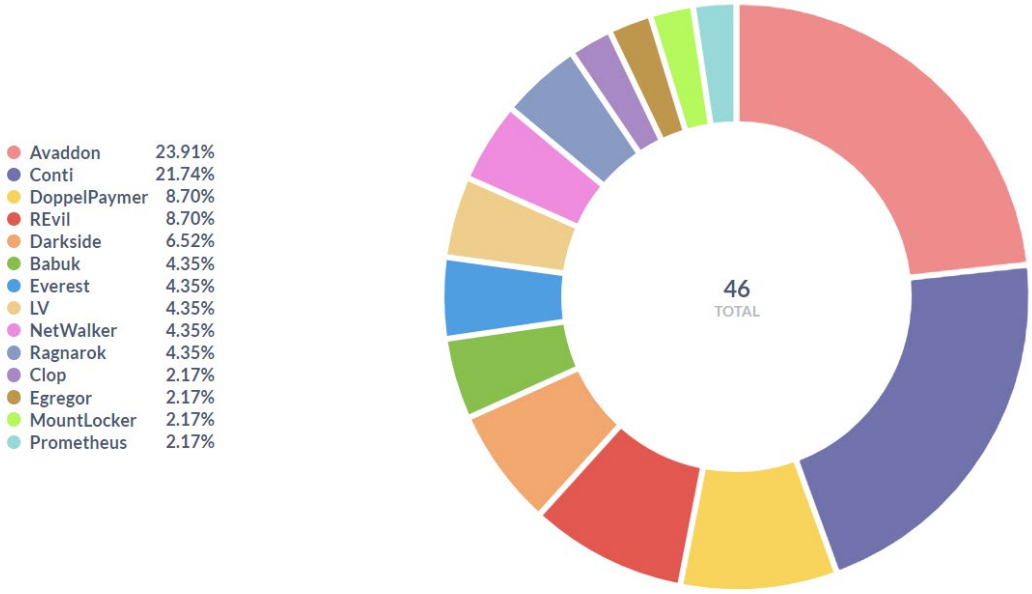
Victim industries in France correlate with the global dataset, but not exactly. Most notable in our view is the **significantly higher proportion of victims in the 'Finance and Insurance' space.** Retail, in the meantime, features much less. Of the 42 Finance Industry victims we have recorded, 14% were in France. Canada also represented 14% of this dataset while the US leads with 42%. The pattern here therefore **appears to be that other industries in France have been impacted less, rather than that Finance has been impacted more.** This dataset is small, however, and probably cannot be read into too deeply.

In terms of a distribution across business size, victim demographics in France mirror the global pattern almost exactly.



Victims in France are overwhelmingly small businesses

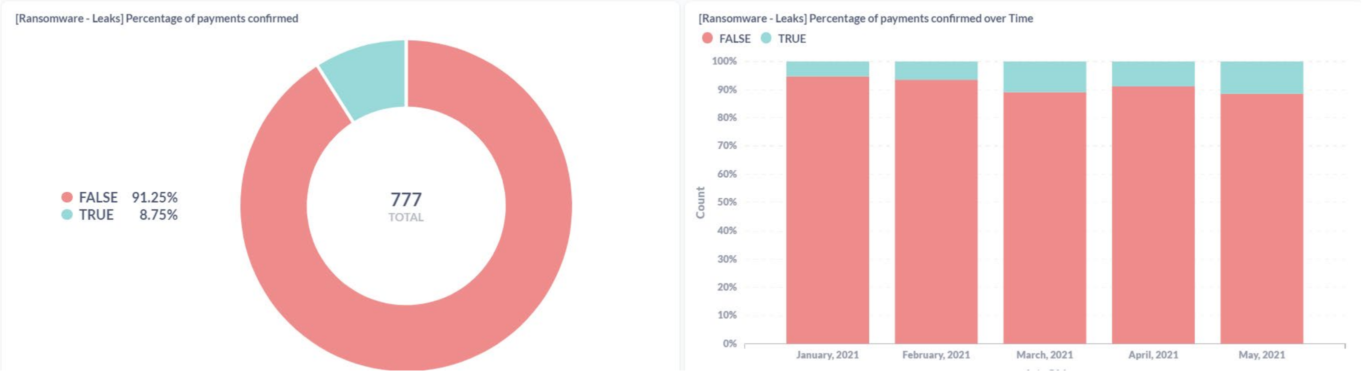
The distribution of attacks across threat actors in France tracks the global trend very closely also.



The distribution of actors in France matches global patterns

Payment

It is difficult to track payment exactly, as the outcome of negotiations is often opaque to us, but from the cases where we have been able to deduce with confidence that a payment was made, we observe that somewhat less than 10% of victims actually pay, even once they have been threatened on a leak site.



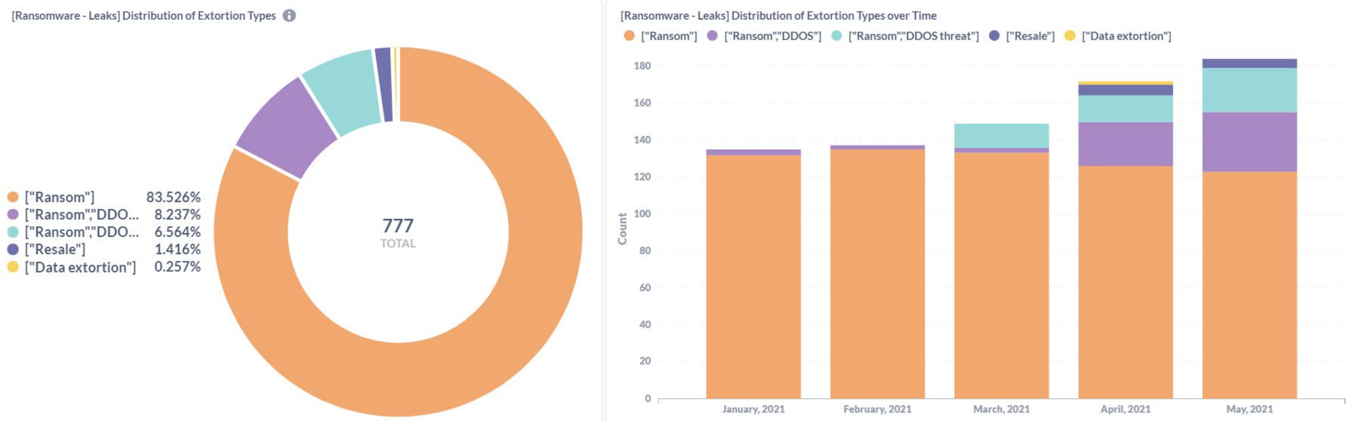
Our deductions suggest that less than 10% of named victims actually pay

In their recent Data Breach Investigations Report[3], Verizon observes that “**90% of ransomware incidents that did not result in any loss**”. This data could be telling the story that organizations are no longer paying the ransoms. But we must also keep in mind that this Verizon loss data includes individuals as well as organizations, which is another potential reason for the numbers being smaller. As

[3] https://verizon.com/dbir/

Verizon emphasizes: “Unfortunately, we do not have a sufficient level of detail to distinguish between the two”.

Extortion Techniques



Pure encryption and ransom now account for only 83.5% of extortion techniques

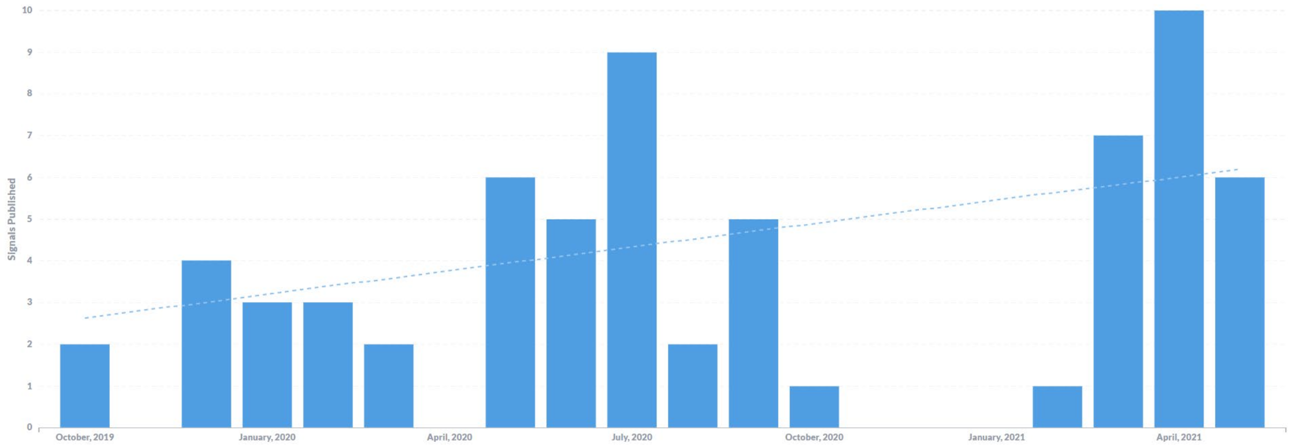
An important and concerning trend to note is the growing frequency of other forms of coercion and monetisation in the cases we observe. **More than 15% of all the observable extortion cases now involve other forms of extortion, like DDoS, or the resale of the stolen data to other markets.**

The lesson for us from this trend is that **we cannot afford to think of this problem purely through the lens of ‘ransomware’.** This is an extortion crime, and we predict that criminals will continue adapting new forms of extortion as the threat posed by encryption is mitigated by means of backup.

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. This month we consider again the issue of vulnerabilities and attacks involving security technologies.

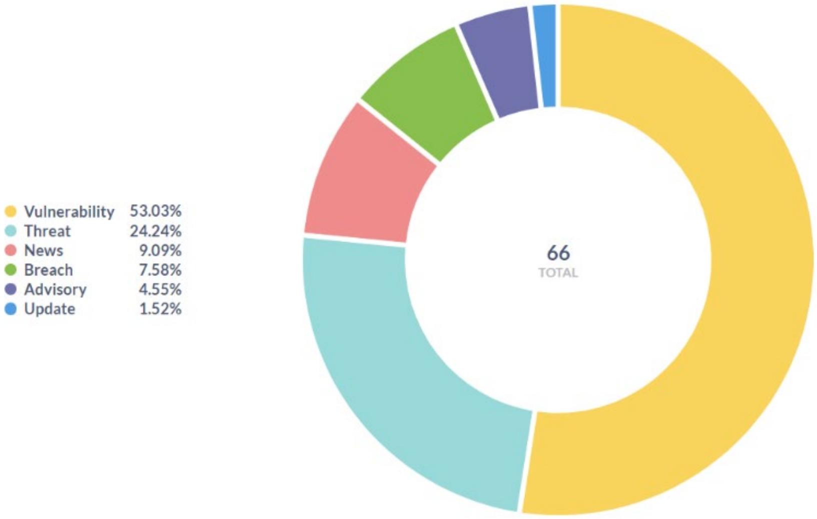
Our analysts assign a specific tag to any Signal that involves issues with security technologies, regardless of the type of Signal. In the graph below you can observe the use of this tag in our advisories over time.



Signals involving issues with security products over time

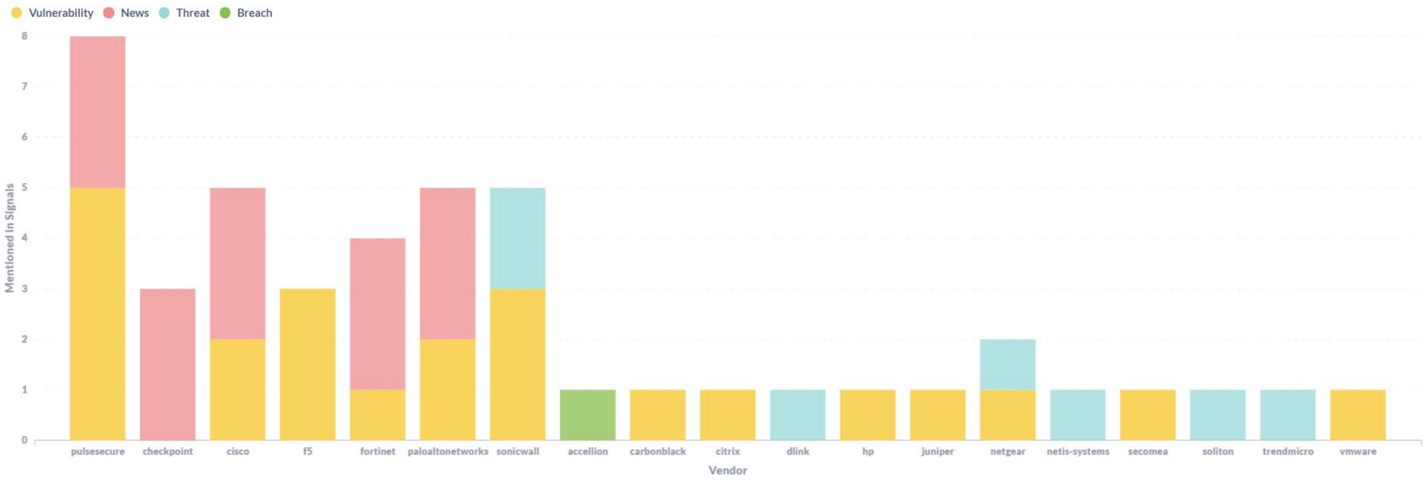
As the graph above illustrates, this issue seems to drift in and out of the security news cycle over time. There was a notable 'peak' in activity over the first wave of COVID lockdowns as VPN technologies were being especially targeted, but that petered off toward the end of 2020.

The last three months have shown a marked acceleration, however. This 2021 trend peaked in April with a new monthly high but has persisted somewhat in May. Overall, the increased prevalence of this theme in our World Watch advisories is clear to see.



Most of the Signals involving security products involved Vulnerabilities, but 16 reported on Threats

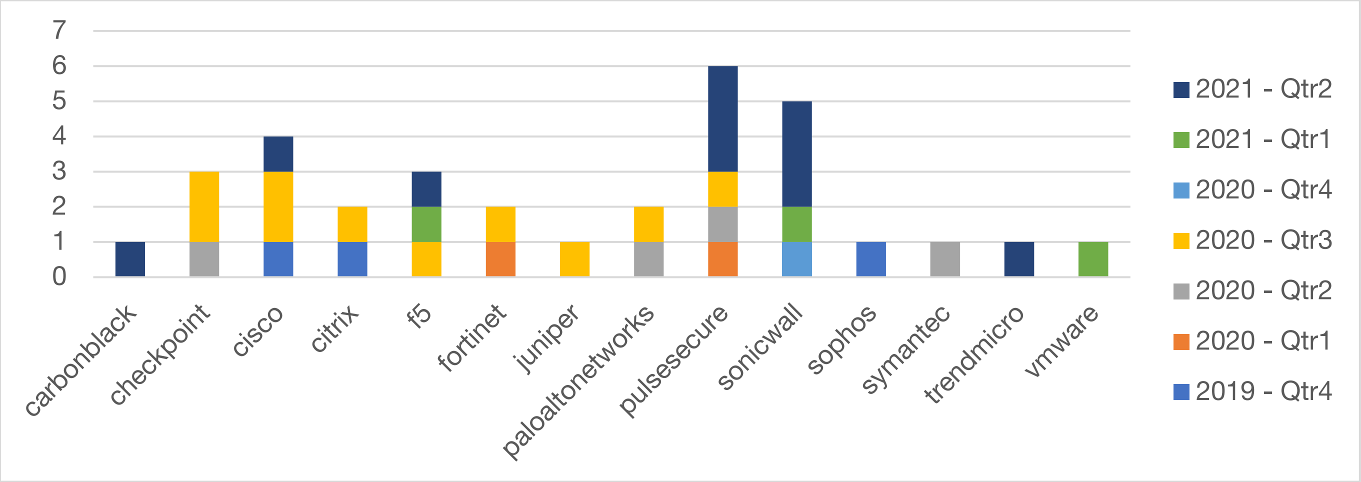
We also tag the specific products referenced in our advisories. When those two tags overlap, the following data emerges:



Security products contributing to this trend in our Signals

It is fair to say that as a security vendor we are particularly attuned to issues involving security technologies, but the data regarding this persistent issue is also clear. Not all mentions of a security product are remarkable, but the vendors listed above were mentioned in specific advisories where **the security technology arguably contributed to the security problem, rather than alleviating it**.

We look at a subset of these technologies to determine how their appearances in our World Watch Signals has shifted over time. Note that there is still a month left in Q2, so the counts for that period will be slightly under reported.



Security products in World Watch Signals over time

It is clear that certain vendors have been in the security news more often in recent times, and some are appearing more often than others in general. But the challenge with vulnerability management is pervasive across several vendors.

These vulnerabilities are actively being exploited by criminals and state-backed groups alike, so this is more than just a theoretical issue.

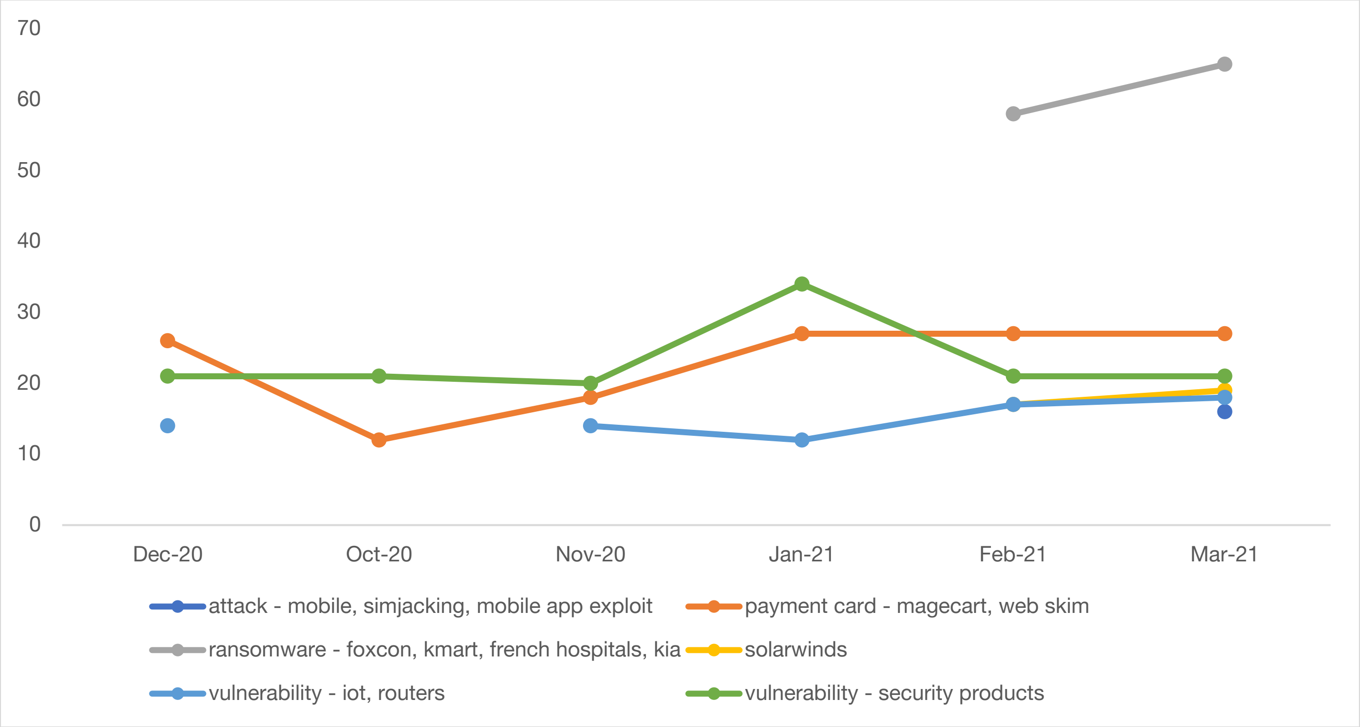
Topic Modeling (Beta)

We continue to experiment and evolve the capabilities of the Topics section in the Monthly Report. One aspiration is to use Machine Learning to help identify trends and topics. We have already introduced 'Topic Modelling', which is an algorithm to group similar bodies of text together based on word frequency and use. Topic modelling does not have any context nor is it capable of making sense of the words.

In the April 2021 report we used the topic modelling algorithm to highlight certain patterns based on topics found in preceding topics we extracted. We built on this idea to see if we cannot find a programmatic means to achieve the same with less manual evaluation.

Summary

The result of these efforts is a view of the trends emerging from our Signals, based on the content of the advisories, rather than their categorization or tags. We filter that output down to a selection of more interesting groupings to produce the following:



Topics over time as determined by our ML algorithms

By examining the groups presented by the algorithm, and observing their trajectory over time, we can make the following observations.

1. A specific variety of Signals discussing **extortion attacks emerged as a significant theme in March**, and grew even more prominent in April, with 65 Signals being grouped under this heading
2. The **group of Signals involving security products** grew in February but then shrunk a bit in March. It has remained consistently present as a grouping over the last six months, however.
3. A group of Signals involving **online card skimming and 'Magecart' attacks** grew toward the end of 2020 and has remained constant since then, with 27 Signals grouped under this heading. This is a topic that does not receive enough attention in our view.

4. A group of Signals dealing with **vulnerabilities in IoT and home routers** disappeared after October but emerged again at the end of 2020 and has grown since then to include 18 Signals.
5. **SolarWinds** emerged as a theme at the start of the year and has grown to include 19 Signals.
6. The theme of **mobile-related attacks** emerged for the first time in April (shown in the March column) and contains 16 Signals.

How we do it.

We start by calculating an intersection of topics extracted for the current month and the preceding month. We select sets that intersect with 50% or more words. Each set has 20 words and with the 50% threshold we will keep the intersection and label it based on the words and the Signals associated with the two sets used in the calculation. These resultant sets will be our baseline.

The Apr-May 2021 baseline consists of 42 topic sets that intersect on half or more of the topic words. A unique label was assigned to each set and falls into one of the following main categories:

- Vulnerability
- Attack
- Data leak
- Ransomware
- Payment card
- Phishing
- COVID-19
- Password
- SolarWinds
- Research
- Campaign
- Bypass
- TTP (Tactics Techniques Procedures)
- Android (Strong Android only category)

These categories are subdivided to be more specific for a unique grouping. The ‘Vulnerability’ category is by far the most common category with all its variations, followed by ‘Attack’.

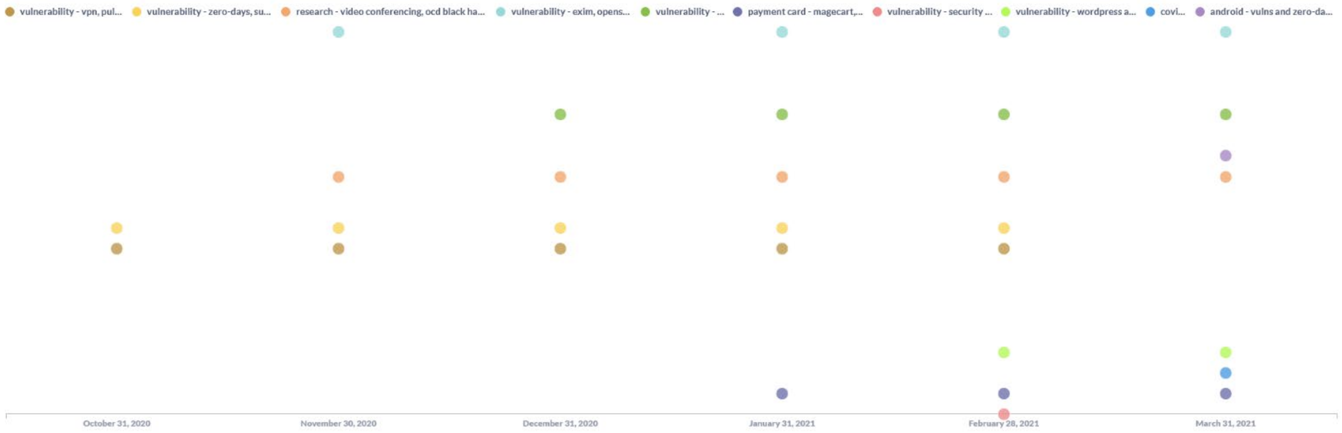
Next, we use the baseline and calculate an intersection using topic sets for each month not included in the baseline calculation. This means that we omit the current month and the month before from the following calculation. For each month we iterate the baseline and calculate the intersection for each topic set for the given month. In this case we retain all intersections that match 100%. These fully matched sets will be part of our trend thread. The 100% threshold is very conservative and will minimize any accidental overlap.

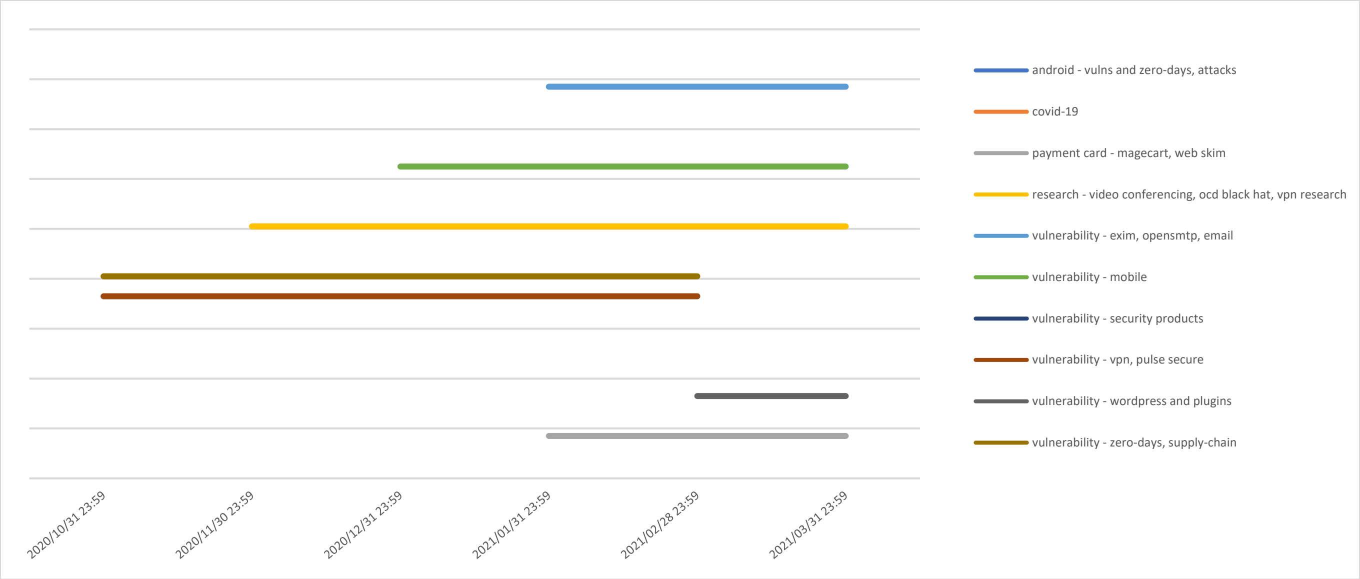
To see how this plays out we did the following. We used topics from May 2021 and April 2021 to calculate the baseline. Next, we use the baseline and calculate the topic intersection for each month starting at October 2021 and we repeated this approach through March 2021.

This resulted in only 10 trend threads out of a possible 42. The legend of the graph is unfortunately not clear due to a limitation of our graphing framework. From left to right the labels read:

- Vulnerability – VPN, Pulse Secure
- Vulnerability – Zero-days, Supply-chain
- Research – Video conferencing, OCD Black Hat, VPN Research

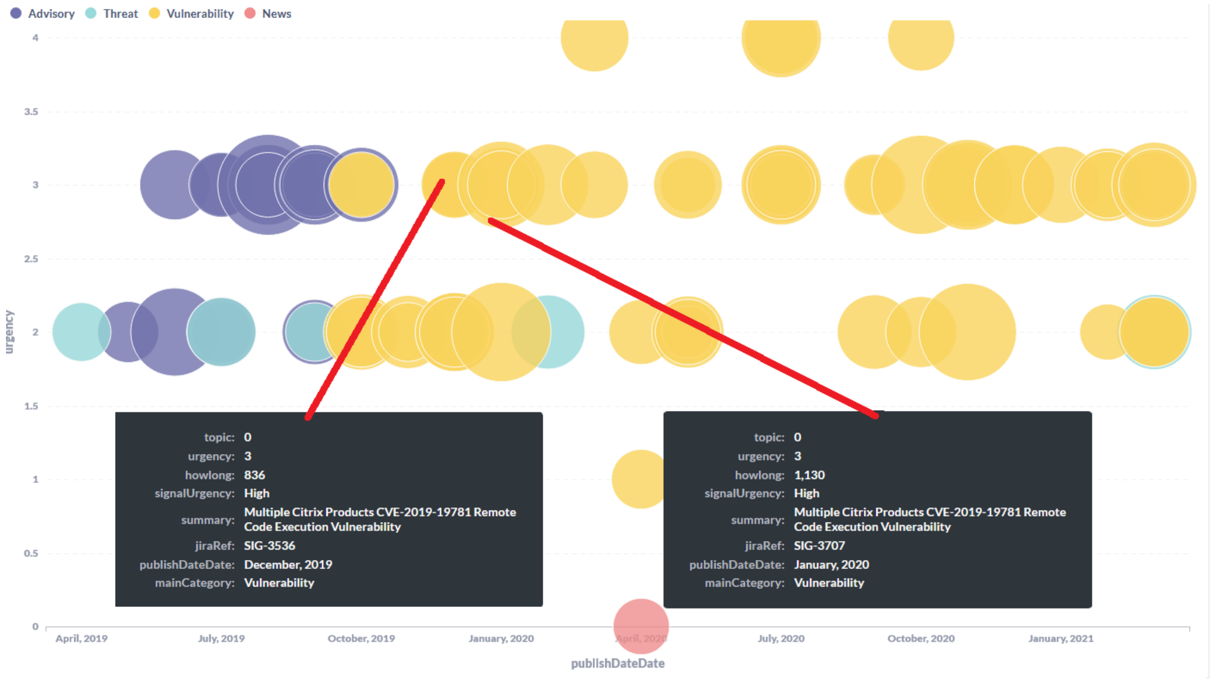
- Vulnerability – Exim, OpenSMTP, Email
- Vulnerability – mobile
- Payment Card - Magecart, web skim
- Vulnerability – Security Products
- Vulnerability – WordPress and plugins
- Covid-19
- Android – Vulns and zero-day, attacks





Notice that there are two groups that start on October 31, 2020, and are present up to February 28, 2021, then suddenly drop off. Upon analysis it was found that the 'Vulnerability – Zero-days, Supply-chain' labelled thread consists of a handful of Signals associated with Citrix, Tomcat, Ghostcat, and QNAP vulnerabilities. As of March 31, 2021, the Signals previously associated have now been split off into three separate groupings.

The Citrix Signals that were included in the now missing 'Vulnerabilities – zero-days, supply-chain' label were pulled into a larger topic grouping involving vulnerabilities.

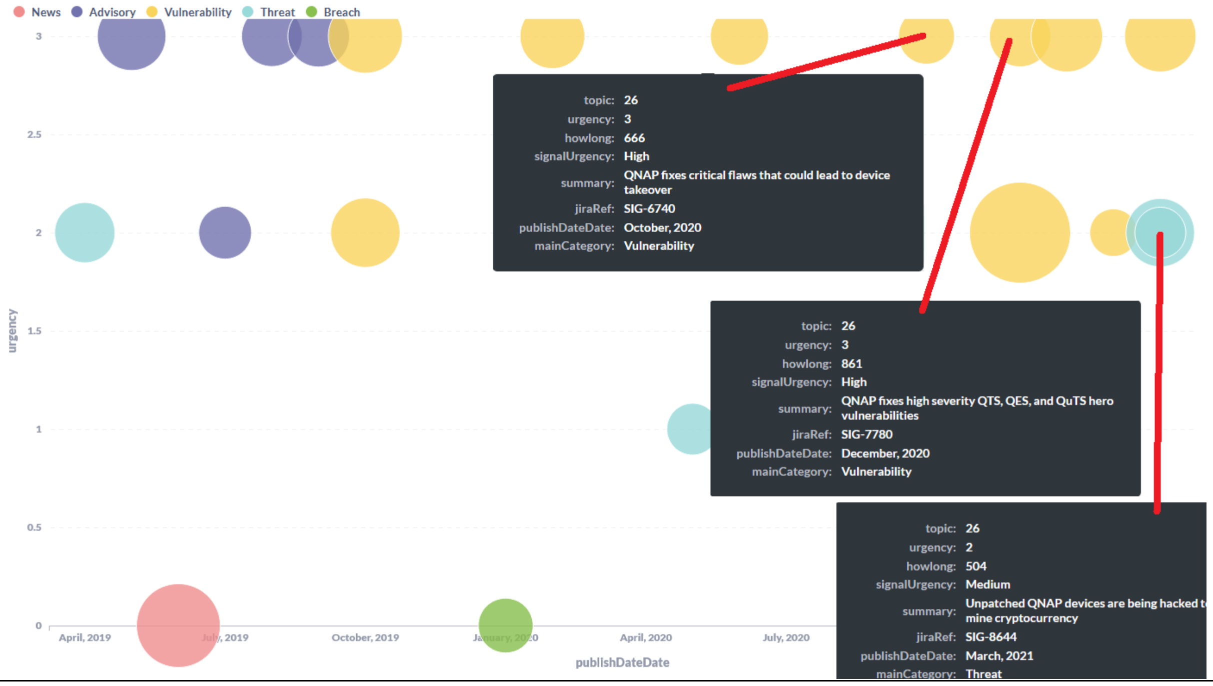


topic: 0
urgency: 3
howlong: 836
signalUrgency: High
summary: Multiple Citrix Products CVE-2019-19781 Remote Code Execution Vulnerability
jiraRef: SIG-3536
publishDateDate: December, 2019
mainCategory: Vulnerability

topic: 0
urgency: 3
howlong: 1,130
signalUrgency: High
summary: Multiple Citrix Products CVE-2019-19781 Remote Code Execution Vulnerability
jiraRef: SIG-3707
publishDateDate: January, 2020
mainCategory: Vulnerability

Also missing from the ‘Vulnerabilities – zero-days, supply-chain’ labelled group are Signals involving QNAP. These were pulled into one group that has evolved to become a cluster of several IoT vulnerabilities including QNAP devices.

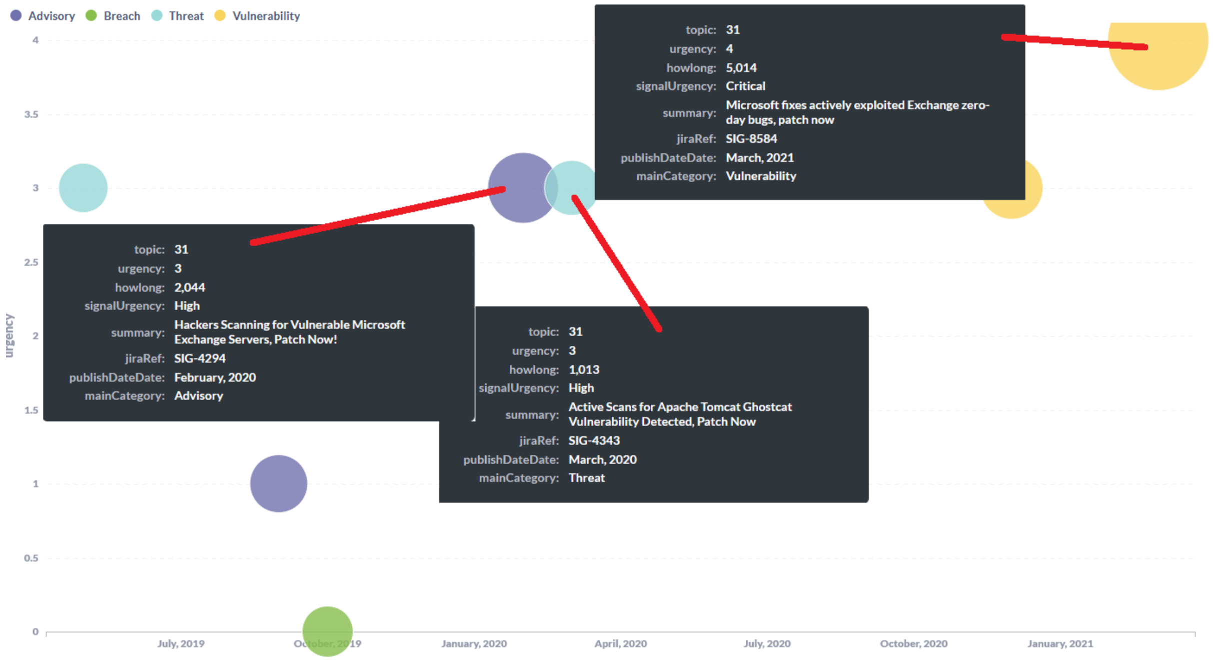
Keeping with the missing ‘Vulnerability – Zero-days, Supply-chain’ label, the Apache Ghostcat Signal was included with other Signals that cover stories where attackers were actively scanning for vulnerable applications:



topic: 26
urgency: 3
howlong: 666
signalUrgency: High
summary: QNAP fixes critical flaws that could lead to device takeover
jiraRef: SIG-6740
publishDateDate: October, 2020
mainCategory: Vulnerability

topic: 26
urgency: 3
howlong: 861
signalUrgency: High
summary: QNAP fixes high severity QTS, QES, and QuTS hero vulnerabilities
jiraRef: SIG-7780
publishDateDate: December, 2020
mainCategory: Vulnerability

topic: 26
urgency: 2
howlong: 504
signalUrgency: Medium
summary: Unpatched QNAP devices are being hacked t mine cryptocurrency
jiraRef: SIG-8644
publishDateDate: March, 2021
mainCategory: Threat

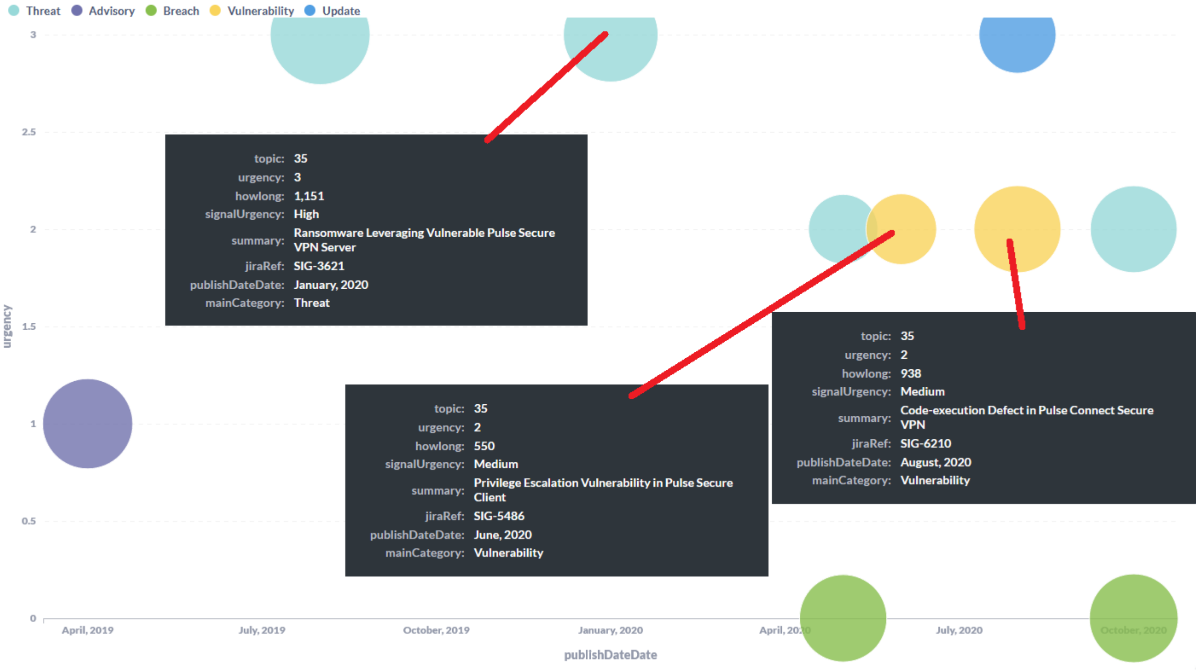


topic: 31
urgency: 4
howlong: 5,014
signalUrgency: Critical
summary: Microsoft fixes actively exploited Exchange zero-day bugs, patch now
jiraRef: SIG-8584
publishDateDate: March, 2021
mainCategory: Vulnerability

topic: 31
urgency: 3
howlong: 2,044
signalUrgency: High
summary: Hackers Scanning for Vulnerable Microsoft Exchange Servers, Patch Now!
jiraRef: SIG-4294
publishDateDate: February, 2020
mainCategory: Advisory

topic: 31
urgency: 3
howlong: 1,013
signalUrgency: High
summary: Active Scans for Apache Tomcat Ghostcat Vulnerability Detected, Patch Now
jiraRef: SIG-4343
publishDateDate: March, 2020
mainCategory: Threat

The missing ‘Vulnerability – VPN, Pulse Secure’ trend label can be ascribed to the conservative threshold requirement of a 100% match with the baseline. For March 2021, the match was 93.3% and this resulted in the missing label.

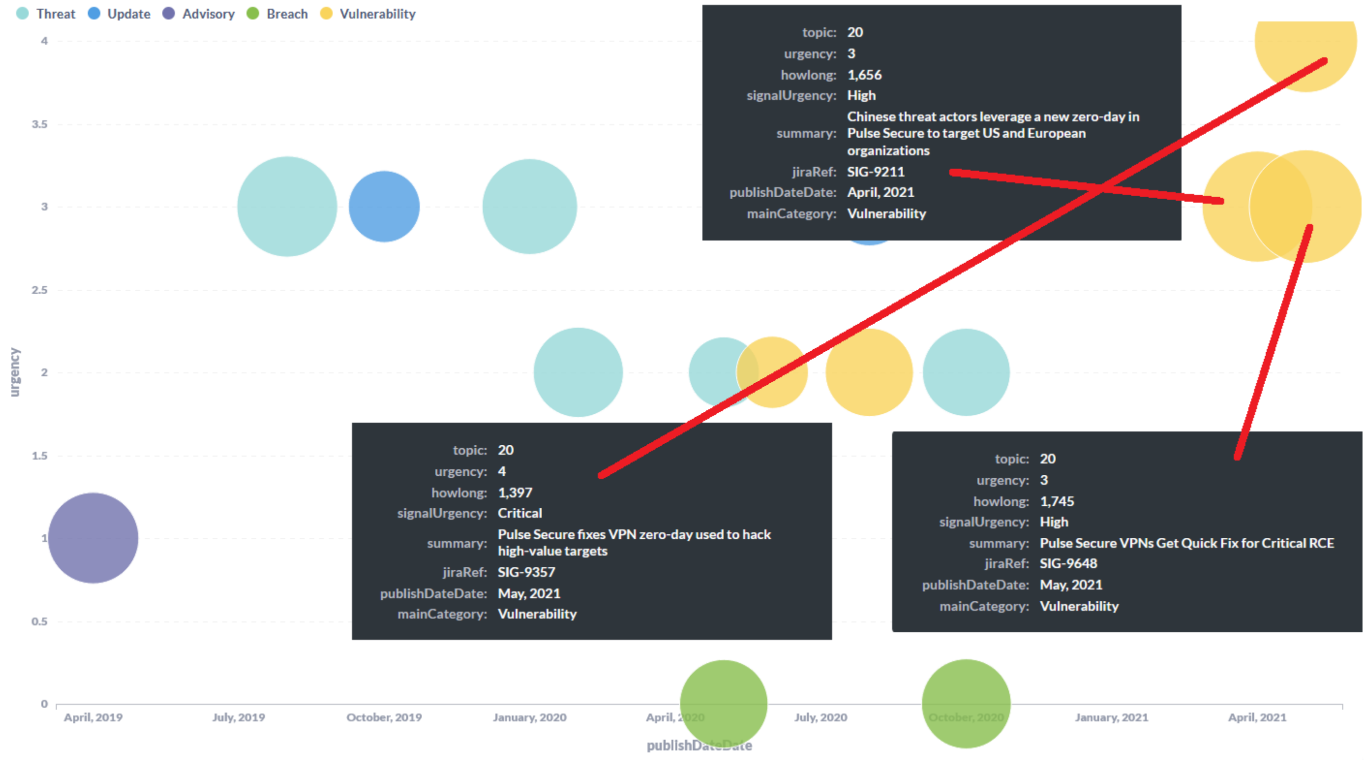


topic: 35
urgency: 3
howlong: 1,151
signalUrgency: High
summary: Ransomware Leveraging Vulnerable Pulse Secure VPN Server
jiraRef: SIG-3621
publishDateDate: January, 2020
mainCategory: Threat

topic: 35
urgency: 2
howlong: 550
signalUrgency: Medium
summary: Privilege Escalation Vulnerability in Pulse Secure Client
jiraRef: SIG-5486
publishDateDate: June, 2020
mainCategory: Vulnerability

topic: 35
urgency: 2
howlong: 938
signalUrgency: Medium
summary: Code-execution Defect in Pulse Connect Secure VPN
jiraRef: SIG-6210
publishDateDate: August, 2020
mainCategory: Vulnerability

While on the topic of VPNs we want to refer to our closing remark in the Topic section of the April 2021 report. We see that **attackers, especially state-affiliated, have made a point of targeting popular security products.** When evaluating the Signal SIG-9211 we can see that this was a prelude to SIG-9648.



topic: 20
urgency: 3
howlong: 1,656
signalUrgency: High
summary: Chinese threat actors leverage a new zero-day in Pulse Secure to target US and European organizations
jiraRef: SIG-9211
publishDateDate: April, 2021
mainCategory: Vulnerability

topic: 20
urgency: 4
howlong: 1,397
signalUrgency: Critical
summary: Pulse Secure fixes VPN zero-day used to hack high-value targets
jiraRef: SIG-9357
publishDateDate: May, 2021
mainCategory: Vulnerability

topic: 20
urgency: 3
howlong: 1,745
signalUrgency: High
summary: Pulse Secure VPNs Get Quick Fix for Critical RCE
jiraRef: SIG-9648
publishDateDate: May, 2021
mainCategory: Vulnerability

This wraps up this section, but there is still some work that must be done to increase the scope of topics included in our trend thread. **Please stay tuned** and see how we evolve this capability.

Good News Cyber

This month we started this new section to spread some positivity and share news stories that focus less on doom and gloom. We want to celebrate the success and progress of efforts by law enforcement and those working in the cybersecurity community all with a focus on creating a safer society.

We have covered incidents involving scams as well as Business Email Compromise (BEC) in the past. Law enforcement agencies in the Asia Pacific (APAC) region have stepped up to confront these threats. SecurityWeek's Ionut Arghire reports that **Interpol intercepted more than $83 million in fraudulent money transfers** as part of operation codename HAECHI-I[4]. This was a three-year project to combat cybercrime in Korea, with participation from authorities in Cambodia, China, Indonesia, Laos, Philippines, Singapore, Thailand, and Vietnam.

The money that was intercepted was linked to investment fraud, money laundering involving illegal online gaming, online sextortion, romance scams, and voice phishing. Over 1,600 bank accounts worldwide were frozen and a total of 892 cases were solved. Authorities arrested 585 individuals as part of this exercise.

Staying with the APAC region, Ionut reports, **Microsoft created a Cybersecurity Council to boost public-private response against cyberattacks in the APAC region**[5]. Policy makers and influencers from Korea, Malaysia, Brunei, Philippines, Indonesia, Singapore, and Thailand will be members of the Asia Pacific Public Sector Cybersecurity Executive Council. The purpose of the council is to improve cooperation, improve communication, and share technology and threat intelligence.

Authorities in Mexico have arrested Florian Tudor, a Romanian citizen, at the request of Romanian authorities for murder, blackmail, and human trafficking. A Mexican judge must still rule on the Romanian extradition request.

Tudor is believed to be the leader of the "Riviera Maya Gang" that is linked to ATM skimming and payment card fraud in Mexico[6]. Tudor created a business to service ATMs specializing in the new Intacash ATMs. The gang is believed to have stolen nearly $1.2 billion from victims using approximately 100 ATMs across Mexico. Tudor managed to bribe Mexican politicians and law enforcement agents investigating ATM fraud cases.

Brazil's government passed stricter legislation regarding digital crimes.[7] More stringent penalties were instated for device invasion, theft, and misconduct in digital media environments, as well as crimes committed through manipulation or social engineering techniques involving emails, social networks, instant messaging apps.

Staying with the Americas, we revisit the **Executive Order (EO) titled 'Executive Order on Improving the Nation's Cybersecurity' that President Biden issued** in response to the numerous cyberattacks against the USA.[8] We do not doubt that the SolarWinds supply-chain attack was the catalyst that forced the USA government to issue a formal and coordinated response. We issued an advisory in SIG-9480 that highlights key aspects of the EO.

[4] https://www.securityweek.com/interpol-says-585-people-arrested-apac-operation-against-cyber-enabled-crime

[5] https://www.securityweek.com/microsoft-creates-cybersecurity-council-public-sector-apac

[6] https://krebsonsecurity.com/2021/05/boss-of-atm-skimming-syndicate-arrested-in-mexico/

[7] https://www.zdnet.com/article/brazil-approves-stricter-legislation-to-tackle-online-crime

[8] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

This EO has the potential to help stem the tide of mounting cyber-attacks, not just in the United States, but it also raises the minimum bar for cyber defense and compliance everywhere. One such area is supply-chain verification and we highlighted this in SIG-8510 that noted another EO signed by President Biden to review supply-chain security.

Supply-chain encompasses a broad spectrum of domains. Focusing just on computing, we can see that any software vendor, hardware vendor, or service provider that wish to do business with the US government will need to step up their game. This can have a knock-on effect to third parties and perhaps further. It also has the potential to accelerate the 'Balkanization' or fragmentation of the business landscape.

Balkanization, historically, has its roots in the continuous colonization of the central European and Balkan region. Applying this concept to business and technology we will see a future unfold where certain nations will prescribe what technology businesses can use. This has already been observed in how China has responded to the West's treatment of Huawei. The supply-chain review process can potentially drive divisions even further.

The software bill of materials (SBOM) is a method of describing the components of software. Some components are proprietary and created by the vendor, while others are borrowed from libraries provided by tech vendors or open source and freely available. The SBOM will require vendors to show diligence in their review of their software libraries and dependencies. Vendors will also have to be able to provide a SBOM to a potential client interested in the product. The SBOM can be valuable for managing vulnerability disclosures and planning threat models to determine risk exposure.

Another welcomed requirement specified in the EO is the endorsement of zero trust principles. These principles will require extra effort for those seeking to implement controls that are designed around the seven zero trust tenants defined by NIST. [9] These can be summarized as verify each transaction explicitly based on authenticated and authorized sessions, assume breach thus forcing the operators to constantly monitor and inspect resources for compromise, and apply the concept of least privilege everywhere.

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

DATA BREACHES

Ransomware attacks were the leading cause of breaches and data leaks in our stories this month. Attacks have not shown signs of subsiding and the groups behind these operations are becoming more brazen and successful. They were seen targeting the healthcare, technology, and energy sectors and governments alike.

We followed up on one supply-chain compromise we mentioned in April 2021. The Codecov supply-chain compromise was used by attackers to gain access to some source code repositories and credentials of Rapid7. Like a supply-chain compromise, Fujitsu's "ProjectWEB" tool was compromised, and attackers used it to steal customer data.

Data breaches due to misconfiguration and human error are still making the news, but ransomware related ones overshadowed them this month.

Stolen ParkMobile data is now free for wannabe scammers

Date: 03 May 2021

The account information for almost 22 million ParkMobile customers is now in the hands of hackers and scammers after the data was released for free on a hacking forum.

Ryuk Ransomware Attack Sprung by Frugal Student

Date: 07 May 2021

The student opted for “free” software packed with a keylogger that grabbed credentials later used by "Totoro" to get into a biomolecular institute.

Largest U.S. pipeline shuts down operations after ransomware attack

Date: 10 May 2021

Colonial Pipeline, the largest fuel pipeline in the United States, has shut down operations after suffering what is reported to be a ransomware attack.

Ransomware attack on healthcare admin company CaptureRx exposes multiple providers across United States

Date: 11 May 2021

Multiple healthcare providers across the United States are reporting being impacted by a ransomware attack on CaptureRx, a San Antonio-based company providing drug-related administrative services.

Rapid7 source code, credentials accessed in Codecov supply-chain attack

Date: 14 May 2021

US cybersecurity firm Rapid7 has disclosed that some source code repositories were accessed in a security incident linked to the supply-chain attack that recently impacted customers of the popular Codecov code coverage tool.

Manchester City Council leaks vehicle number plate in parking ticket spreadsheet

Date: 14 May 2021

Manchester City Council exposed online the number plates of more than 60,000 cars slapped with parking tickets, breaking data protection laws.

Toshiba Tec France hit by DarkSide

Date: 14 May 2021

The Toshiba unit, which sells self-checkout technology and point-of-sale systems to retailers, revealed that the incident occurred on the evening of May 4.

Babuk ransomware group dumps D.C. Police data

Date: 14 May 2021

The posted police files include documents on crimes, suspects, investigations, and copies of three months’ worth of the daily intelligence briefings given to police chief Robert Contee III. There are also extensive documents from the department’s human resources branch, including hiring initiatives, leave requests, and letters of reinstatement for officers returning to the department.

Ireland’s Health Services hit with $20 million ransomware demand

Date: 17 May 2021

Ireland's health service, the HSE, says they are refusing to pay a $20 million ransom demand to the Conti ransomware gang after the hackers encrypted computers and disrupted health care in the country.

23 Android apps exposed data for millions of users

Date: 21 May 2021

A report released by Check Point Research said they have discovered 23 Android apps on the Google Play Store that expose users' sensitive data online.

Air India data breach impacts 4.5 million customers

Date: 24 May 2021

Air India disclosed a data breach after personal information belonging to roughly 4.5 million of its customers was leaked two months following the hack of Passenger Service System provider SITA in February 2021.

Audio maker Bose discloses data breach after ransomware attack

Date: 25 May 2021

Bose Corporation (Bose) has disclosed a data breach following a ransomware attack that hit the company's systems in early March.

Japanese government agencies suffer data breaches after Fujitsu hack

Date: 27 May 2021

Offices of multiple Japanese agencies were breached via Fujitsu's "ProjectWEB" information sharing tool. Fujitsu states that attackers gained unauthorized access to projects that used ProjectWEB, and stole some customer data.

MALWARE AND EXPLOITS

We reported on two technical ransomware related stories this month. One ransomware variant was observed with a new worm like capability and a Remote Access Trojan (RAT) was observed with a module that fakes ransomware attacks.

Unlike most months, we reported on one proof-of-concept exploit being released, and in this case, for a wormable vulnerability. Fortunately, Windows did release a patch for the bug in their monthly patch Tuesday updates.

In an interesting development, one of the Magecart groups performing online card skimming attacks was observed using server-side malicious code in addition to client-side code. This is unusual because these attacks usually use JavaScript code and not PHP.

Loader malware, with the general purpose of downloading and installing additional malware on a machine, received some attention from us this month. New loaders, Snip3 and WastedLoader, were observed being spread via phishing attacks and browser exploit kits respectively.

Revealing the ‘Snip3’ Crypter, a Highly Evasive RAT Loader

Date: 12 May 2021

Morphisec released details of a highly evasive piece of malware that is being spread using phishing attacks with the ultimate goal of installing a Remote Access Tool on the victim machine.

Exploit released for wormable Windows HTTP vulnerability

Date: 18 May 2021

Proof-of-concept (PoC) exploit code has been released for a wormable vulnerability in the latest Windows 10 and Windows Server versions.

Magecart Goes Server-Side in Latest Tactics Changeup

Date: 18 May 2021

The latest Magecart iteration, Magecart Group 12, is finding success with a new PHP web shell skimmer.

A New Watering Hole, Oldsmar and a Botnet

Date: 19 May 2021

Dragos discovered a Florida water utility contractor hosting malicious code on their website, known as a watering hole attack, while investigating the water poisoning attempt against the city of Oldsmar, Florida.

New malware campaign called WastedLoader targets unpatched IE browsers

Date: 20 May 2021

Bitdefender has published a report on a new campaign using RIG Exploit Kit to target unpatched Internet Explorer web browsers. The attack exploits two old unpatched Internet Explorer browser vulnerabilities (CVE-2019-0752 and CVE-2018-8174).

XingLocker, a MountLocker variant, gets new worm capabilities

Date: 20 May 2021

MountLocker is a Ransomware-as-a-Service (RaaS), active since July 2020, which is constantly improving its capabilities with more sophisticated scripting and anti-prevention features. The last added feature presumably allows the ransomware to use enterprise Windows Active Directory APIs to "worm through networks". But we could not verify this claim in any of the recent MountLocker samples we found. The source confirmed it's in another close variant called XingLocker we have not reversed yet.

Microsoft: Massive malware campaign delivers fake ransomware

Date: 21 May 2021

A massive malware campaign pushed the Java-based STRRAT remote access trojan (RAT), known for its data theft capabilities and the ability to fake ransomware attacks.

Nobelium Phishing Campaign Poses as USAID

Date: 31 May 2021

Microsoft uncovered the SolarWinds crooks using mass-mail service Constant Contact and posing as a U.S.-based development organization to deliver malicious URLs to more than 150 organisations.

VULNERABILITY MANAGEMENT

Like last month, in May we learned of several zero-days being actively exploited in the wild. The affected technologies being Pulse Secure SSL VPN, iOS, macOS, tvOS, Android, and Adobe Acrobat. Fortunately, patches have been released.

Microsoft had a busy month, featuring three times with their monthly patches, a report on 25 vulnerabilities in IoT/OT devices, and with a proof-of-concept exploit being released for PatchGuard.

Several other vendors released a slew of patches for general vulnerabilities in their products. These were SonicWall, Hewlett Packard Enterprise, Dell, Cisco, Exim and Pulse Secure to name a few. Numerous patches were for vulnerabilities that could allow an unauthenticated remote attacker to execute arbitrary code on a vulnerable system. This type of vulnerability is a popular target for hackers attempting to breach a corporate network.

VMware featured twice, releasing security fixes for two vulnerabilities that could be exploited remotely without credentials. One of these we classified as 'Critical' severity.

Microsoft Warns 25 Critical Vulnerabilities in IoT, Industrial Devices

Date: 03 May 2021

Researchers from Microsoft's Section 52 team who focus on IoT vulnerabilities recently uncovered several critical memory allocation flaws, collectively tracked as "BadAlloc", affecting multiple IoT and OT devices' OS. The vulnerabilities could be exploited by attackers to bypass security controls to execute malicious code or trigger DoS conditions.

Python also impacted by critical IP address validation vulnerability

Date: 04 May 2021

Python 3.3 standard library 'ipaddress' suffers from a critical IP address vulnerability (CVE-2021-29921) identical to the flaw that was reported in the "netmask" library earlier this year.

Pulse Secure fixes VPN zero-day used to hack high-value targets

Date: 04 May 2021

Pulse Secure has fixed a zero-day vulnerability in the Pulse Connect Secure (PCS) SSL VPN appliance that is being actively exploited to compromise the internal networks of defense firms and govt agencies.

Apple fixes 2 iOS zero-day vulnerabilities actively used in attacks

Date: 04 May 2021

Today, Apple has released security updates that fix two actively exploited iOS zero-day vulnerabilities in the Webkit engine used by hackers to attack iPhones, iPads, iPods, macOS, and Apple Watch devices.

Hewlett Packard Enterprise Plugs Critical Bug in Edge Platform Tool

Date: 04 May 2021

Researchers warned that unpatched versions of HPE's Edgeline Infrastructure Manager are open to remote authentication-bypass attacks.

Vulnerable Dell driver puts hundreds of millions of systems at risk

Date: 05 May 2021

A driver that's been pushed for the past 12 years to Dell computer devices for consumers and enterprises contains multiple vulnerabilities that could lead to increased privileges on the system.

Critical 21Nails Exim bugs expose millions of servers to attacks

Date: 05 May 2021

Newly discovered critical vulnerabilities in the Exim message transfer agent (MTA) software allow unauthenticated remote attackers to execute arbitrary code and gain root privilege on mail servers with default or common configurations.

VMware fixes critical RCE bug in vRealize Business for Cloud

Date: 06 May 2021

VMware has released security updates to address a critical severity vulnerability in vRealize Business for Cloud that enables unauthenticated attackers to remotely execute malicious code on vulnerable servers.

Cisco bugs allow creating admin accounts, executing commands as root

Date: 06 May 2021

Cisco has fixed critical SD-WAN vManage and HyperFlex HX software security flaws that could enable remote attackers to execute commands as root or create rogue admin accounts.

Qualcomm Chip Bug Opens Android Fans to Eavesdropping

Date: 07 May 2021

A malicious app can exploit the issue, which could affect up to 30 percent of Android phones.

Microsoft May 2021 Patch Update

Date: 12 May 2021

The May 2021 security update contains fixes for 55 vulnerabilities, with four classified as Critical, 50 as Important, and one as Moderate. Three patched zero-day vulnerabilities were publicly disclosed but not known to be used in attacks.

Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader

Date: 12 May 2021

A patch for Adobe Acrobat, the world’s leading PDF reader, fixes a vulnerability under active attack affecting both Windows and macOS systems that could lead to arbitrary code execution.

Vulnerabilities nicknamed FRAGATTACKS affect most devices with WiFi enabled

Date: 13 May 2021

Mathy Vanhoef has discovered new vulnerabilities in the Wi-Fi standard and its implementation in most Wi-Fi products. Collectively these vulnerabilities affect all Wi-Fi security protocols since the launch of the wireless network technology in 1997. Protocols from WEP to WPA3 are affected.

May Android security updates patch 4 zero-days exploited in the wild

Date: 20 May 2021

According to info provided by Google's Project Zero team, four Android security vulnerabilities were exploited in the wild as zero-day bugs before being patched earlier this month.

Apple fixes three macOS, tvOS zero-day bugs exploited in the wild

Date: 25 May 2021

Apple has released security updates to patch three zero-day vulnerabilities that attackers might have exploited in the wild.

Pulse Secure VPNs Get Quick Fix for Critical RCE

Date: 26 May 2021

One of the workaround XML files automatically deactivates protection from an earlier workaround: a potential path to older vulnerabilities being opened again.

VMware warns of critical bug affecting all vCenter Server installs

Date: 26 May 2021

VMware urges customers to patch a critical remote code execution (RCE) vulnerability in the Virtual SAN Health Check plug-in and impacting all vCenter Server deployments.

Asahi Linux Dev Reveals ‘M1RACLES’ Flaw in Apple M1

Date: 28 May 2021

A flaw in the design of the Apple Silicon “M1” chip allows any two applications running under an OS to covertly exchange data between them, without using memory, sockets, files, or any other normal operating system features. This works between processes running as different users and under different privilege levels, creating a covert channel for surreptitious data exchange.

SonicWall urges customers to 'immediately' patch NSM On-Prem bug

Date: 31 May 2021

SonicWall urges customers to 'immediately' patch a post-authentication vulnerability impacting on-premises versions of the Network Security Manager (NSM) multi-tenant firewall management solution.

HPE Fixes Critical Zero-Day in Server Management Software

Date: 31 May 2021

The bug in HPE SIM makes it easy as pie for attackers to remotely trigger code, no user interaction necessary.

A new weakness has been discovered in Microsoft PatchGuard

Date: 31 May 2021

A new proof of concept has been published for a vulnerability in Microsoft PatchGuard.

NOTEWORTHY

PortDoor Espionage Malware Takes Aim at Russian Defense Sector

Date: 04 May 2021

According to a report from the Cybereason Nocturnus team, threat actors have been observed targeting Russian-based defense contractors involved in the design of the Russian Navy's nuclear submarines.

AXA pledges to stop reimbursing ransom payments for French ransomware victims

Date: 11 May 2021

One of Europe’s biggest insurers is now suspending policies in France that reimburse victims for ransomware payments.

Train firm’s ‘worker bonus’ email is actually cybersecurity test

Date: 11 May 2021

West Midlands Trains workers discover email promising one-off payment is ‘phishing simulation test’.

Biden issues executive order to increase U.S. cybersecurity defenses

Date: 14 May 2021

President Biden signed an executive order Wednesday to modernize the US's defenses against cyberattacks and give more timely access to information necessary for law enforcement to conduct investigations.

DarkSide cyber extortion group bags over $9 million

Date: 14 May 2021

Sources report that chemical distribution company Brenntag paid $4.4 million ransom and that Colonial Pipeline Company paid approximately $5 million in a bid to obtain a file decryption mechanism and to keep leaked data from going public.

Popular Russian hacking forum XSS bans all ransomware topics

Date: 14 May 2021

One of the most popular Russian-speaking hacker forums, XSS, has banned all topics promoting ransomware to prevent unwanted attention.

ExaGrid may have paid 50 BTC thus $2.6 million in ransom to Conti gang

Date: 19 May 2021

ExaGrid, an American disk-based backup hardware company has presumably been hit by a ransomware attack and paid the ransom estimated to 50 BTC, or $2.6 million, to get its data back. This was revealed in chat logs from May 12th between the cybercriminals and the company. it was targeted by the famous and very active Conti ransomware group.

Orange Cyberdefense Presents at RSA Conference 2021

Date: 20 May 2021

New resources! Charl van der Walt & Wicus Ross presented their talk "All Your LAN are Belong to Us. Managing the Real Threats to Remote Workers." at RSA Conference 2021. Supporting materials, including a comprehensive solutions whitepaper, are available for you to download.