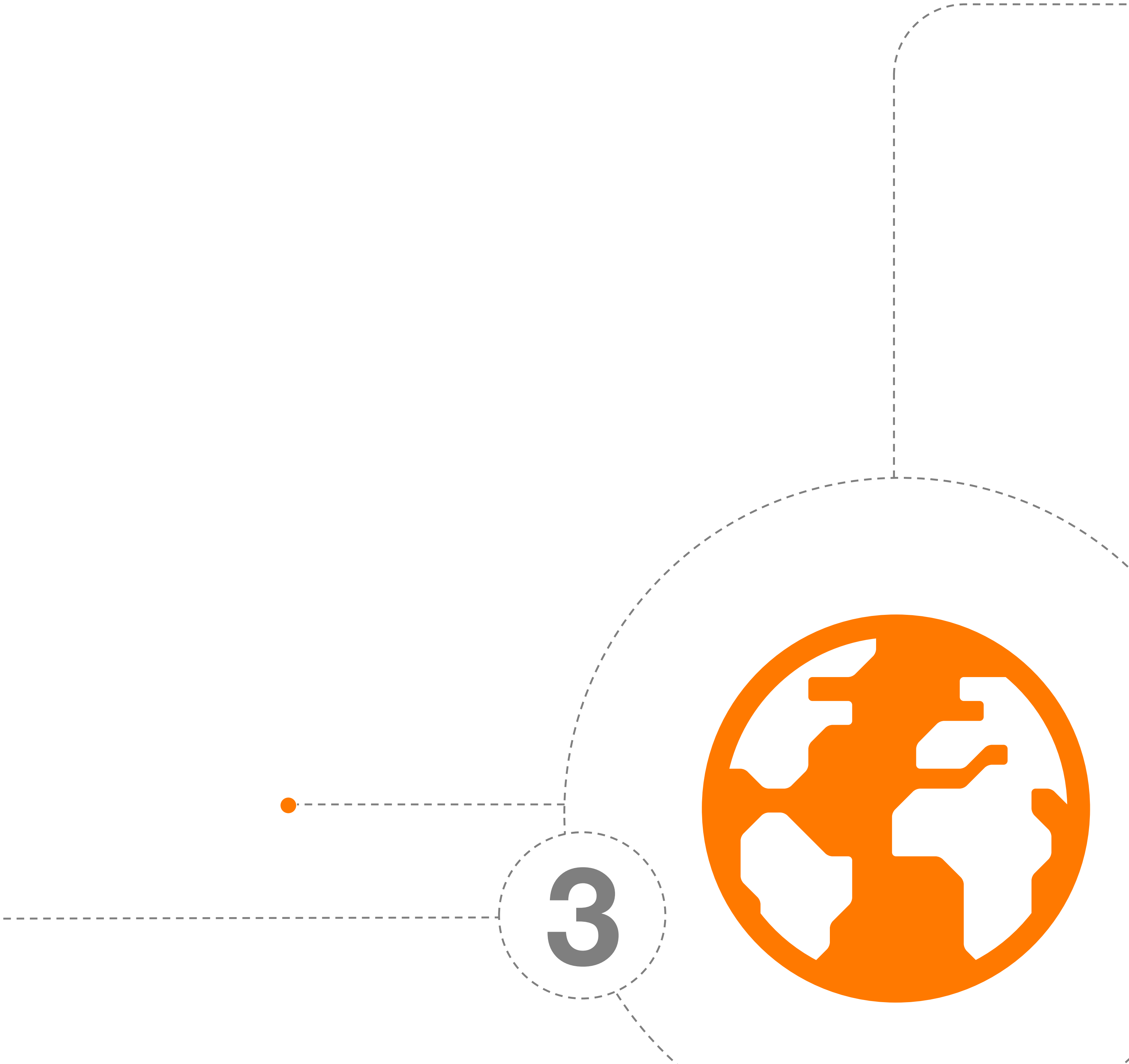
Orange
Cyberdefense

World Watch | Threat Intelligence Report

orange™

Monthly Report
March 2021



CONTENTS

CONTENTS 2

INTRODUCTION 5

OVERVIEW 6

Categories – Monthly Breakdown 7

Services Affected 9

Technologies Affected 10

Breach Trends 13

Our Recommendations 15

Ransomware Trends (Beta) 17

Topics (Beta) 22

General Trends 23

DATA BREACHES 25

Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance 25

Cybersecurity firm Qualys likely latest victim of Accellion hacks 25

SITA data breach affects millions of travellers from major airlines 25

Norway parliament data stolen in Microsoft Exchange attack 25

Hacker dumps Guns.com database with customers, admin data 25

Mimecast: SolarWinds Attackers Stole Source Code 25

Acer reportedly targeted with $50 million ransomware attack 25

Energy giant Shell discloses data breach after Accellion hack 25

Ransomware attack shuts down Sierra Wireless IoT maker 26

CNA insurance firm hit by a cyberattack, operations impacted 26

PHP's Git server hacked to add backdoors to PHP source code 26

FatFace pays out $2 million to Conti ransomware gang 26

Online FX broker FBS leaked 16B customer records via an unsecured server 26

MobiKwik Suffers Major Breach 26

MALWARE AND EXPLOITS 27

Ryuk ransomware now self-spreads to other Windows LAN devices 27

Working Windows and Linux Spectre exploits found on VirusTotal 27

Malicious Code Packages Target Amazon, Lyft, Slack, Zillow 27

Microsoft, FireEye Unmask More Malware Linked to SolarWinds Attackers 27

Hackers hiding Supernova malware in SolarWinds Orion linked to China 27

Unpatched QNAP devices are being hacked to mine cryptocurrency 27

IoT Devices Under Attack By Tor-Based Gafgyt Variant 27

New DEARCRY Ransomware is targeting Microsoft Exchange Servers 28
Google Releases Spectre PoC Exploit For Chrome 28
FBI warns of escalating Pysa ransomware attacks on education orgs 28
Latest Mirai Variant Targets SonicWall, D-Link and IoT Devices 28
Microsoft's Azure SDK site tricked into listing fake package 28
Chinese APT group targets telcos in 5G-related cyber-espionage campaign 28
New APT group SilverFish Has Compromised Thousands of Victims 28
FBI: Phishing emails are spreading this sophisticated malware 28
Hacking group used 11 zero-days to attack Windows, iOS, Android users 28
Hades ransomware targets big firms 28

VULNERABILITY MANAGEMENT 29
Rockwell Automation vulnerability 29
Microsoft fixes actively exploited Exchange zero-day bugs, patch now 29
Google fixes second actively exploited Chrome zero-day bug this year 29
GRUB2 boot loader reveals multiple high severity vulnerabilities 29
Windows DNS SIGRed bug gets first public RCE PoC exploit 29
VMware releases fix for severe View Planner RCE vulnerability 29
Security Patch for Apple Safari Browser 29
Newest Intel Side-Channel Attack Sniffs Out Sensitive Data 30
Microsoft Patch Tuesday Updates Fix 14 Critical Bugs 30
F5 urges customers to patch critical BIG-IP pre-auth RCE bug 30
Netgear fixes 15 vulnerabilities in SOHO switch 30
Vulnerabilities Found in Schneider Electric Power Meters 30
SAP Patches Critical RCE Flaw in Manufacturing Software and More 30
Google Warns Mac, Windows Users of Chrome Zero-Day Flaw 30
Cisco Plugs Security Hole in Small Business Routers 30
GitLab Security Release 30
Two (unconfirmed) critical zero-day flaws in Microsoft Office 365 30
Microsoft Exchange servers now targeted by BlackKingdom ransomware 30
Critical code execution vulnerability fixed in Adobe ColdFusion 31
CISA Warns of Security Flaws in GE Power Management Devices 31
Cisco addresses critical bug in Windows, macOS Jabber clients 31
OpenSSL fixes severe DoS, certificate validation vulnerabilities 31
Apple fixes iOS zero-day vulnerability exploited in the wild 31
Thousands of applications impacted by critical vulnerability in netmask library 31
A vulnerability allowing an attacker to steal credentials on vRealize fixed by VMware 31
Accellion File Transfer Appliance Security Assessment 31

NOTEWORTHY 32
OVH data centre destroyed by fire in Strasbourg 32

Ryuk ransomware hits 700 Spanish government labor agency offices ... 32
Cyber incident at University of the Highlands and Islands ... 32
PPS hit by cyber attack ... 32
Birmingham College Closed After Cyber Attack ... 32
Sky ECC denies police have ‘cracked’ encrypted messaging platform ... 32
Nifty Gateway Digital Art Marketplace Account Compromise ... 32
Australian TV station Channel 9 misses broadcasts after cyber-attack ... 32
New Allegations of Questionable Data Breach Handling by Ubiquiti ... 32

INTRODUCTION

Data breaches are something that we all have become too accustomed to. Unfortunately ignoring the problem is part of the problem. This month we reported on several incidents, most involving some form of digital extortion, where data has been leaked or shared due to error. Ransomware groups are moving to capitalise on this, and we have seen several incidents reported where no malware was deployed to encrypt data, but victims were still harassed for payment.

We featured two stories this month that highlight concern with how some businesses handle data breaches. The first relates to a fintech business in India that has vehemently denied any data breach after a bug bounty researcher reached out to them. The fintech company then publicly lashed out against the bug bounty researcher. The second example is a developing story by Brian Krebs. This story accuses Ubiquiti Networks of grossly mishandling and downplaying the data breach Ubiquiti reported in January 2021.

A rare opportunity presented itself this month that afforded everyone a rare glimpse into the world of a western counterintelligence operation. Google's Project Zero and Threat Analysis Group shared details of two campaigns they disrupted involving 11 zero-days.

This month we saw many serious vulnerabilities bring patches, but for most this was too late as some of these have already been exploited successfully. The Microsoft Exchange ProxyLogon vulnerability featured prominently this month. Attackers had the advantage as they could simply attack exposed and vulnerable Exchange servers, while IT teams scrambled in response. Unsurprisingly ransomware crews moved to capitalise on this.

Several zero-day vulnerabilities were fixed in Google's Chrome and Apple's Safari browsers. Some of the vulnerabilities spanned desktop and mobile platforms. As noted above, some of these were part of state-affiliated attacks.

At a glance

The number of data breaches is increasing and businesses need to prepare for how they will respond to such an eventuality.

Accellion shared a security assessment report produced by Mandiant on the Accellion File Transfer Appliance (FTA). The report highlighted four zero-day vulnerabilities that Accellion fixed. Two important facts are worth mentioning. The first being the presence of a built-in feature of FTA called the 'anomaly detector' that alerted clients to the presence of suspicious files. This was instrumental in identifying the first set of zero-day exploits. The second important fact is that Accellion responded relatively quickly with security fixes. Unfortunately like the Microsoft Exchange ProxyLogon vulnerabilities, the availability of a fix is little consolation when attackers have already exploited the vulnerable service.

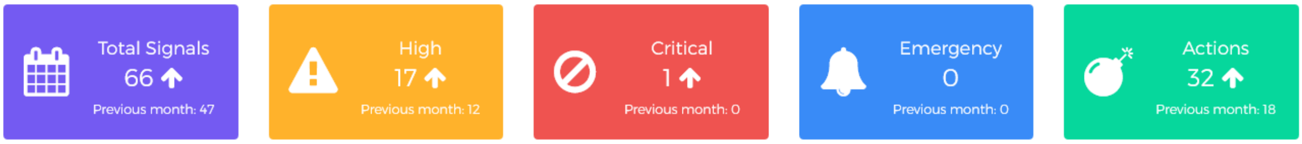
A fire destroyed an OVH data centre in Strasbourg. The fire might have been caused by a faulty uninterrupted power supply that was recently serviced. This incident should remind everyone relying on cloud infrastructure that redundancy does not come automatically with cloud solutions. System design and system deployment must have built-in resilience that can withstand data centre failure.

Law Enforcement Agencies across the globe have been successful in making arrests of prominent cybercrime groups. Their efforts have led to the disruption and subsequent closure of a secure communications provider Sky ECC. Sky sold services that were used by criminals to securely communicate with each other.

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
66 ↑
Previous month: 47

High
17 ↑
Previous month: 12

Critical
1 ↑
Previous month: 0

Emergency
0
Previous month: 0

Actions
32 ↑
Previous month: 18

March 2021 was a busy month for IT and security teams. This can be seen in the number of actions we raised in March 2021. We also hit a new record for most Signals published in a month, namely 66. This is largely due to an increase in our capacity, but there is no doubt that the volume of security events is growing every month.

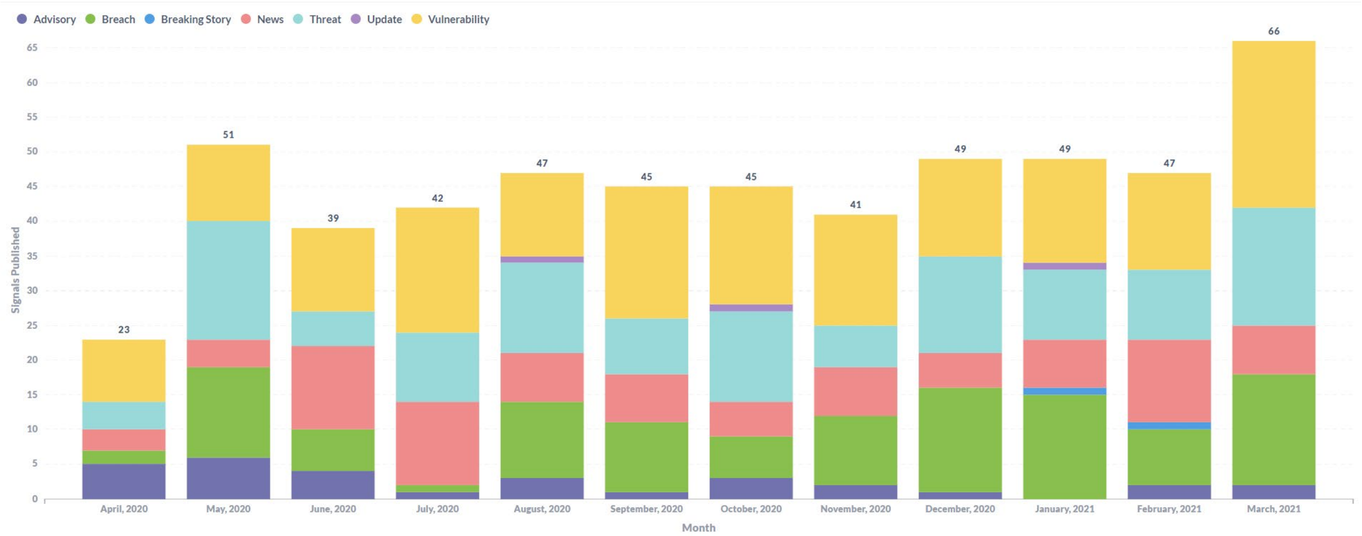
The one 'Critical' Signal we published this month involved the 'ProxyLogon' vulnerability in Microsoft Exchange that we referred to in the introduction. Microsoft released an emergency out-of-band security update for all supported Microsoft Exchange versions that fixed four zero-day vulnerabilities that have been actively exploited in targeted attacks, reportedly by the Chinese state sponsored HAFNIUM group.

The vulnerabilities affect on-premises installations of Exchange Server, Exchange Online is not affected. When used in an attack chain these vulnerabilities allow an attacker to access and steal emails as well as deploy and execute malware to gain further access to the network and steal credentials. There have subsequently been massive attempts to target servers worldwide, by multiple threat groups. The journalist Brain Krebs issued a blog post that claims that "[a]t least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments" have fallen victim to attackers. The global number is believed to reach around 250,000, though these are not official numbers.

The ProxyLogon vulnerabilities and attacks have amazingly stolen the limelight from the SolarWinds incident, though the latter is by no means resolved yet and will no doubt continue to feature in the news and in our reports.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

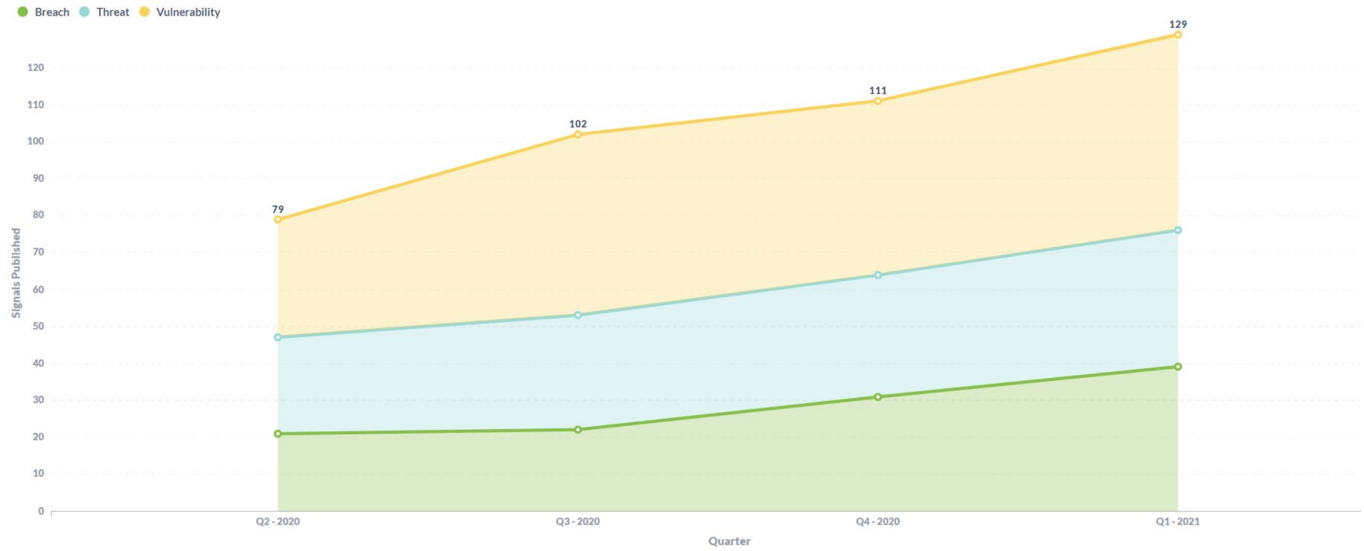


Signals by Category per Month

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

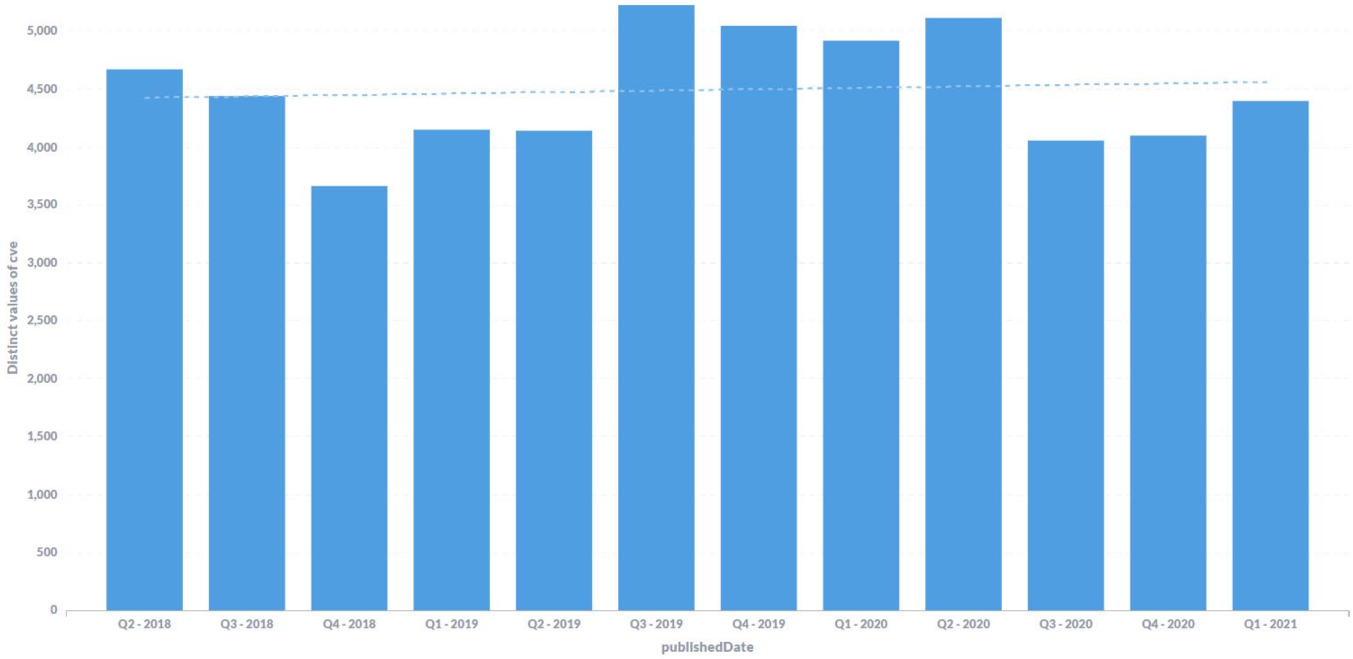
As mentioned previously we hit a new record for the service of 66 Signals published during March. While it is clear that the volumes of Signals have increased across all categories, the reason for this increase may also simply be an increase in our own capacity. We should therefore not read too much into this increase from a security point of view yet.

Despite these internal changes, it is clear that security events in the three key categories – Vulnerabilities, Threats and Breaches have been trending steadily upward over the last four quarters.



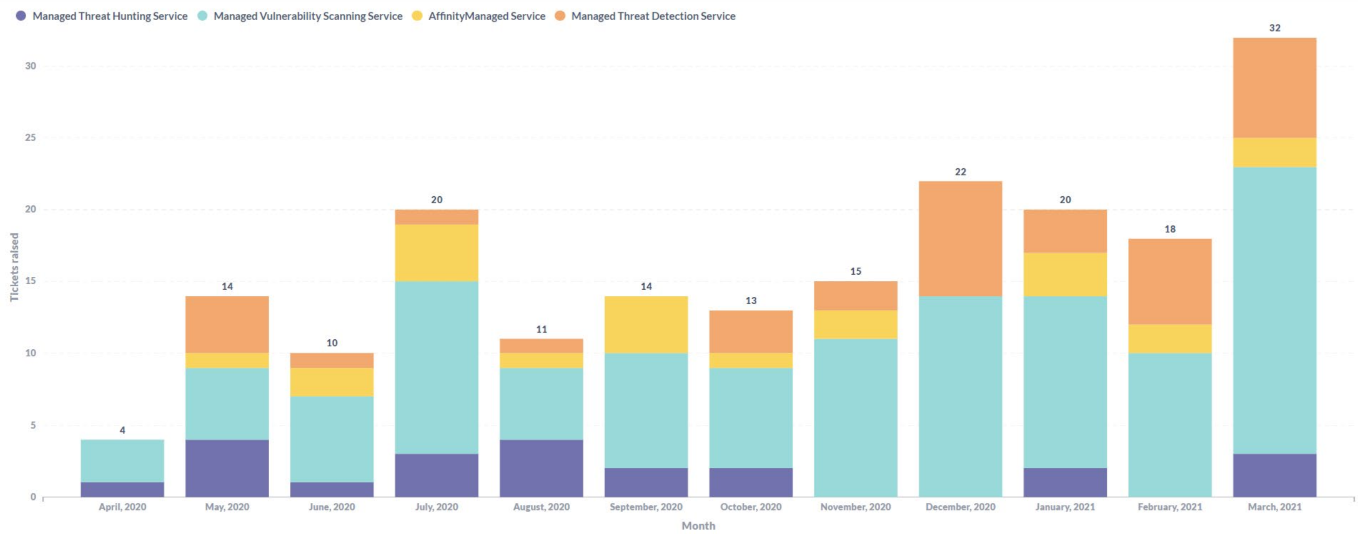
Incidents in all major categories have been trending upwards

The overall volume of vulnerabilities published via the NIST National Vulnerability Database has also be trending upwards slightly over the last 36 months, although Q1 of this year is about average:



Officially recorded vulnerabilities over the last 3 years

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.

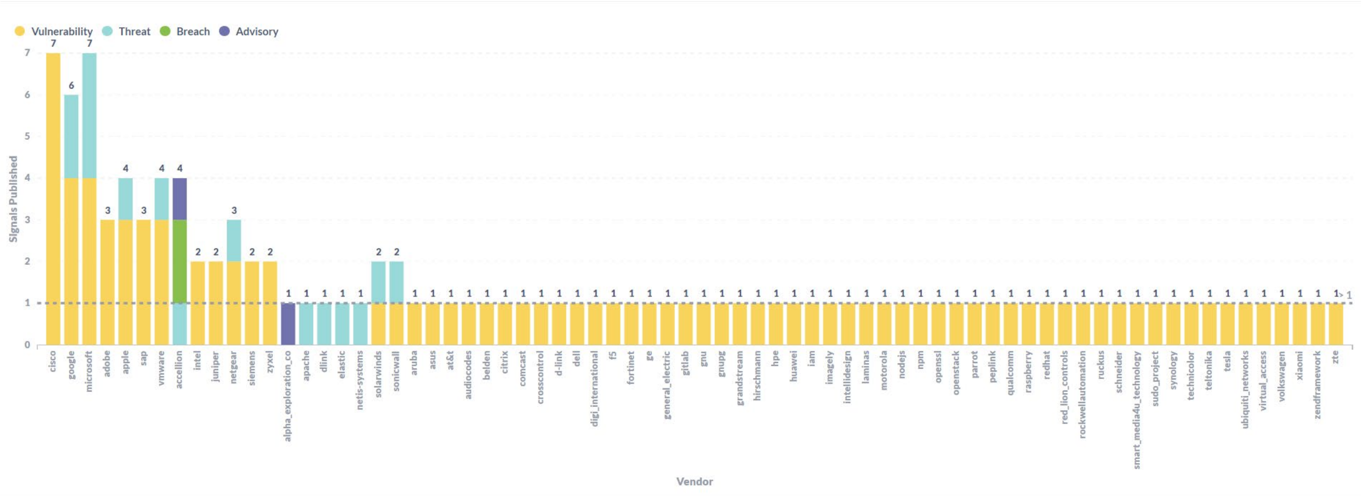
These action requests are recorded by our system and the number of requests raised per month since the beginning is reflected on the graph above. **As would be expected given the Signals volumes for the month, we recorded a record number of tickets with our operations teams, 32 in total. The overall Signals volume doesn't fully explain this increase, however. The March number is a full 50% higher than our previous record for tickets logged, significantly higher than the increase in Signals overall (29%). This reflects just how volatile the security space is becoming and how important it is for us to aware of significant security events and responsive to them when required.**

An examination of the tickets we raised with operations illuminates two interesting themes:

1. The three tickets raised with our Threat Hunting teams all involved threats posed by state-backed APT groups:
   - Microsoft fixes actively exploited Exchange zero-day bugs, patch now
   - Chinese APT group targets telcos in 5G-related cyber-espionage campaign
   - New APT group SilverFish Has Compromised Thousands of Victims
   As we discuss in more detail later in this report, it is becoming abundantly clear that government hacking operations are an ever-present factor in the corporate security landscape and can impact anyone.

2. We dealt with several vulnerabilities impacting security technologies, including f5, Sonicwall, and Accellion. We've remarked on the issue of threats and vulnerabilities involving security technology several times in the past, especially during the 2nd quarter of 2020, after which it appeared to have subsided somewhat. But it seems like this trend may be lifting its head again, as we will examine later in this report.

Technologies Affected



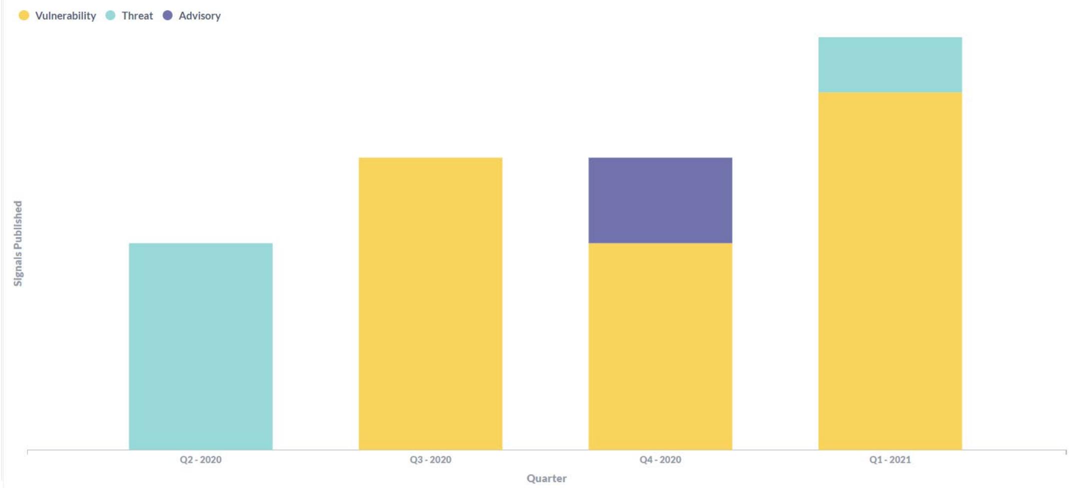
Technologies featuring in our Signals this Quarter

The chart above summarises the technology vendors that were referenced in our Signals across the various categories for **Q1 of 2021**.

Cisco, Google, Microsoft, and Adobe featured highly in the 1st quarter of 2021 as is the norm given the shear scope of their offerings. As always, it's the next 'layer' of vendors that are interesting to consider, those that are featuring less often than the big 4 but have featured more than once in the quarter.

The following observations present themselves:

1. Its notable that the **Apple iOS operating system** has been featuring more and more in our advisories over the last 12 months:



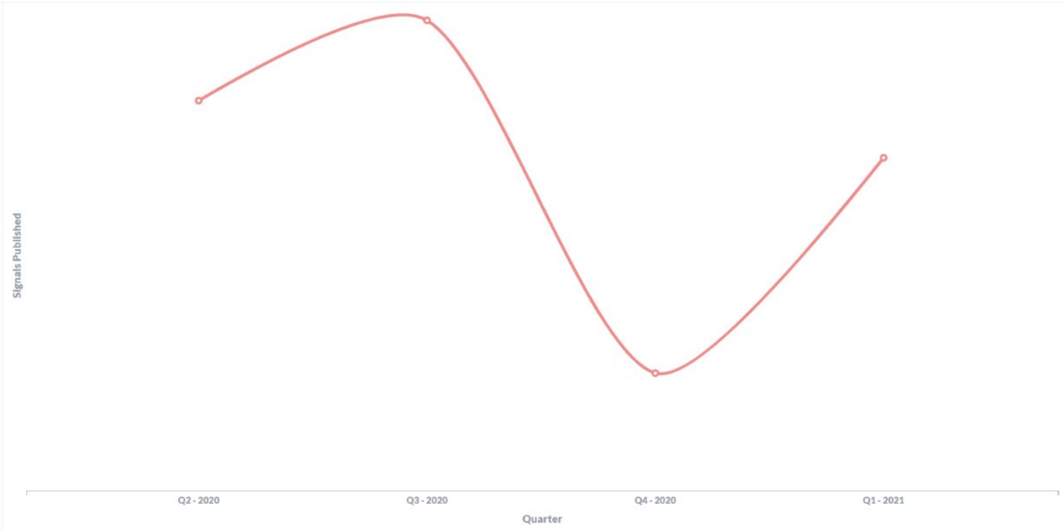
This quarter, the following Signals involved iOS:

- 2021/01/27, Apple fixes another three iOS zero-days exploited in the wild

- 2021/03/09, Security Patch for Apple Safari Browser
- 2021/03/29, Apple fixes iOS zero-day vulnerability exploited in the wild
- 2021/03/30, Hacking group used 11 zero-days to attack Windows, iOS, Android users.

It is clear that vulnerabilities and attacks involving mobile platforms, and even iOS, have become a current variable in our threat models.

2. It appears to us that the trend of **vulnerabilities and exploits impacting security technologies** is tracking upward again, after receding a little at the end of 2020:



The ongoing fallout from the vulnerabilities in the Accellion and the resultant wave 'supply chain' attacks has been a significant driver of this theme in Q1, but other vendors have been impacted also:

- January 14th: **Juniper** January 2021 Security Patch Update
- January 20th: DNSpooq lets attackers poison DNS cache records (**JunOS**)
- February 2nd: **SonicWall** SMA 100 zero-day exploit actively used in the wild
- March 4th: Cybersecurity firm **Qualys** likely latest victim of Accellion hacks
- March 11th: **F5** urges customers to patch critical BIG-IP pre-auth RCE bug
- March 17th: Latest Mirai Variant Targets **SonicWall**, D-Link and IoT Devices
- March 23rd: Energy giant Shell discloses data breach after **Accellion** hack
- March 31st: **VMware** fixes vulnerability allowing an attacker to steal credentials on vRealize

Customers are encouraged to ensure that they have the people and processes in place to respond in a timely manner to vulnerabilities in security vendor products when they're announced, or to engage with a provider that can assist with these functions. There is no doubt that there is a surge in these kinds of vulnerabilities at this time, which, when combined with the apparent rush to deploy or scale remote access capabilities, is leaving critical perimeter security exposed and contributing in a direct way to compromises and breaches.

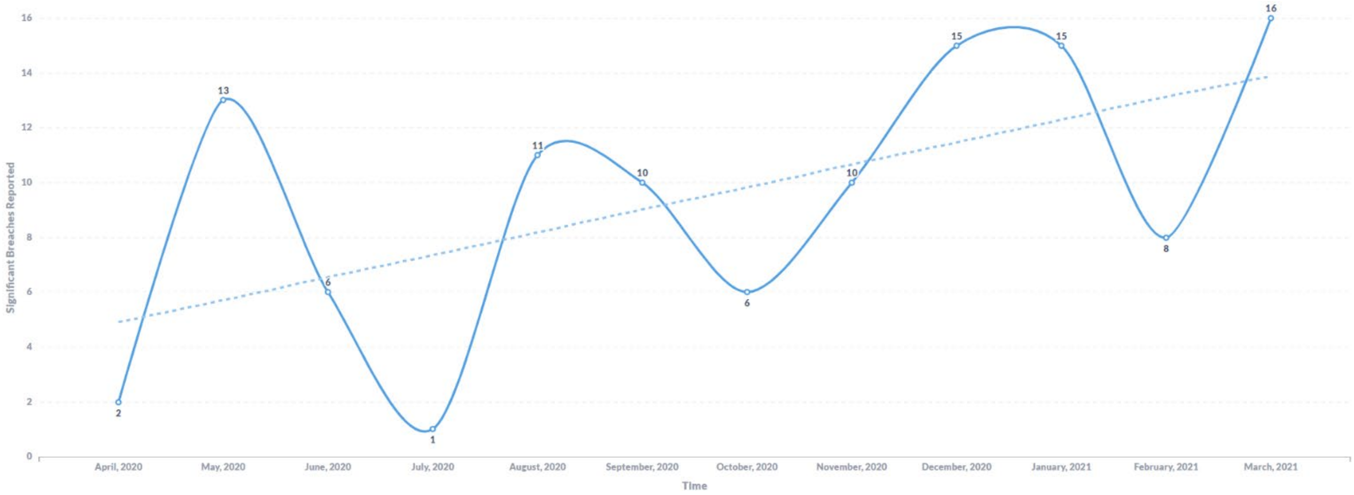
3. We have mentioned **SAP** in Signals 5 times in the last 12 months. 3 of these instances has been in the last quarter. In a recent report published by SAP and security company Onapsis[1] they list 8 vulnerabilities and misconfigurations that are actively being attacked at the moment. According to the report "The window for defenders is significantly smaller than previously thought, with examples

[1] https://therecord.media/sap-systems-usually-come-under-attack-72-hours-after-a-patch/

of SAP vulnerabilities being weaponized in less than 72 hours since the release of patches, and new unprotected SAP applications provisioned in cloud (IaaS) environments being discovered and compromised in less than 3 hours”. Readers are encouraged to review the SAP vulnerability management practices in light of what appears to be an increased focus on this platform and given the apparent agility of attackers the paper describes.

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.

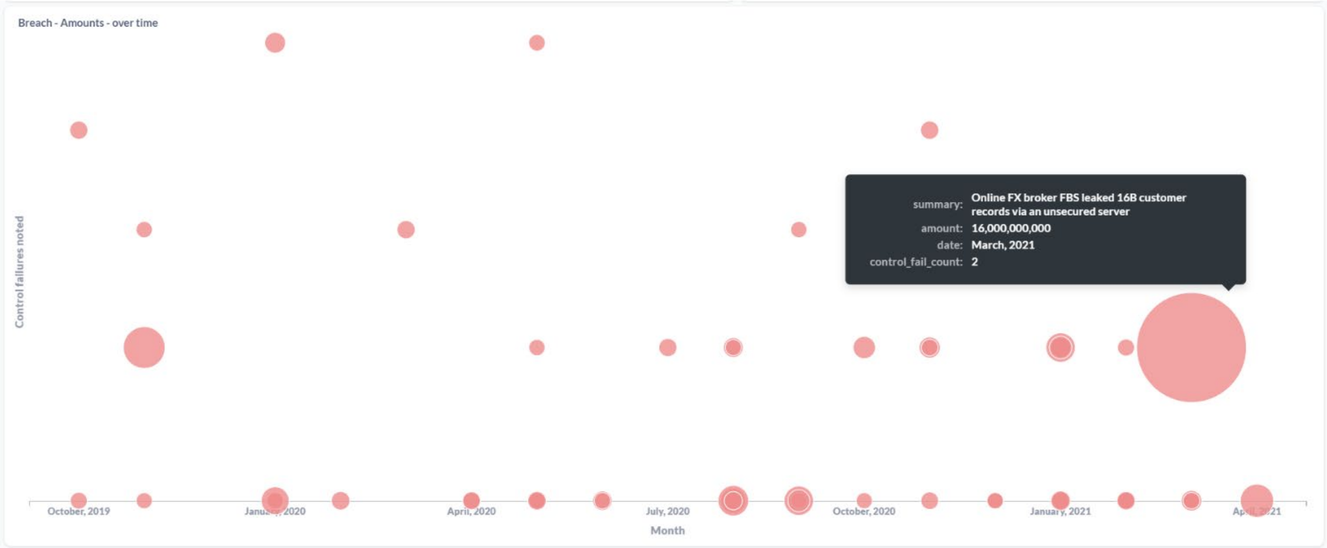


Major breaches recorded over time

The chart above reflects the number of breaches we have reported on per month since the start of the year.

No one was more surprised than we were that we hit yet another record high March this year. If major breaches keep happening at this scale, we may soon reach a point where our own capacity to keep track of these incidents will become the limiting factor in this trend.

Another extraordinary record from March is captured in the chart below, which show, breaches over time and indicates the volume of data lost, and the number of security control failures observed.



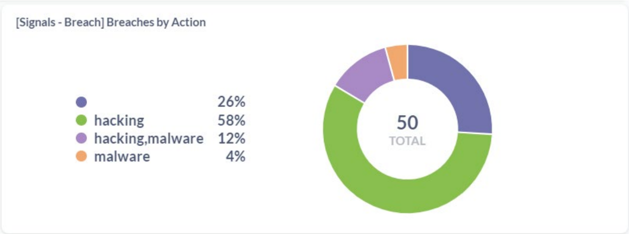
Breaches over time, showing data lost and control failures observed

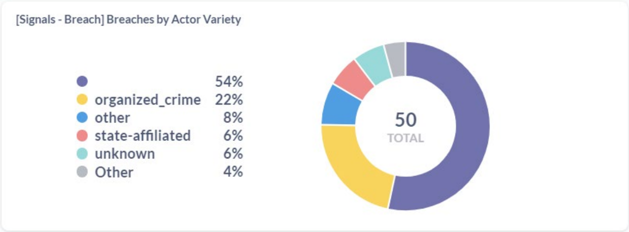
In the chart above each bubble represents a major breach. The X-axis shows time. The Y-axis reflects the number of apparent security control failures that were observed. The size of the bubble reflects the number of records lost in the breach. In March we recorded a wholly unprecedented new record when Online FX broker FBS **leaked 16B customer records** via an unsecured server. The leading foreign exchange broker for online trading, recently left an Elasticsearch server exposed on the Internet that contained over 16 billion data records, including personally identifiable information of its customers.

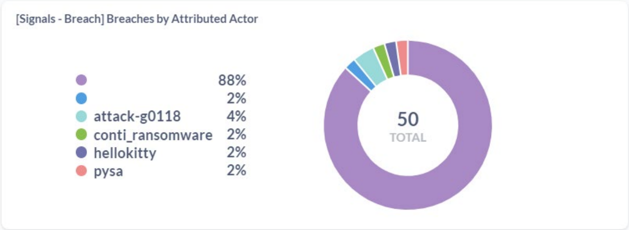
We'll explore the question of security controls and security control failures from our data in the next section. For the FBS breach, we noted and recorded two apparent failures, which are captured in the CIS Top 20 best practice framework as follows:

- **Controlled Access Based on the Need to Know**: Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs) (https://www.cisecurity.org/controls/controlled-access-based-on-the-need-to-know/).

- **Limitation and Control of Network Ports, Protocols and Services**: Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system (https://www.cisecurity.org/controls/limitation-and-control-of-network-ports-protocols-and-services/).







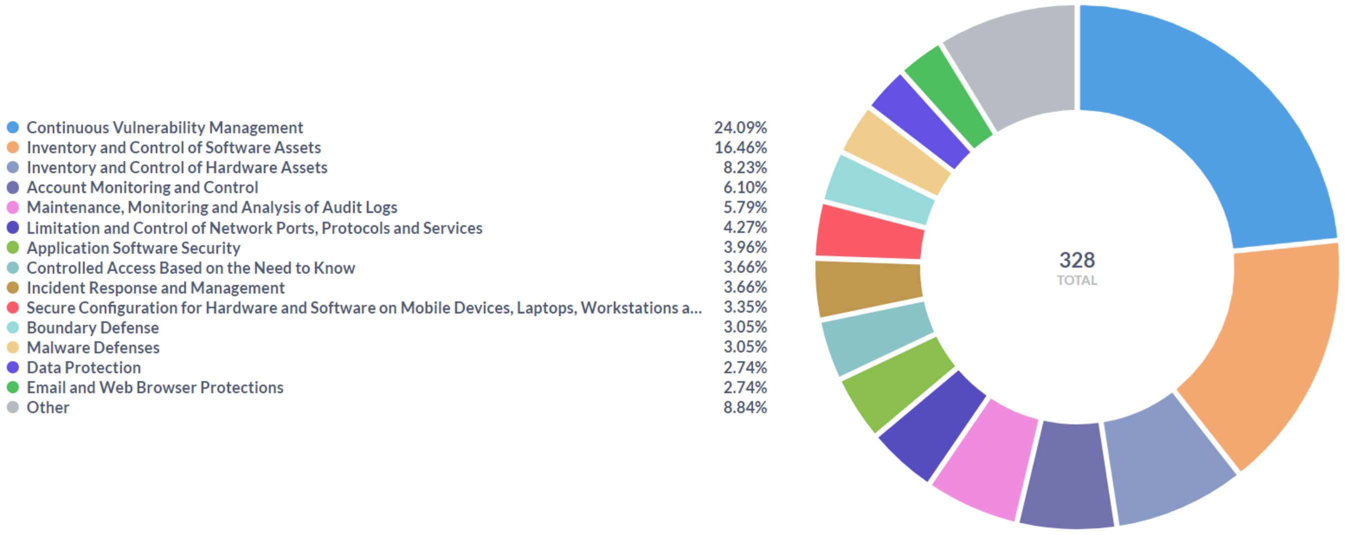
A cursory examination of the major attributes characterising the 50 breaches we recorded this past quarter doesn't reveal anything startling: The majority of the breaches we analysed involved 'traditional' hacking techniques of the type a penetration tester would use. Some include malware also, and a small number (2 this past quarter) involved malware only.

In the majority of cases the actor appears to be related to organized crime, with only 3 breaches being attributed to apparently state-backed actors this past quarter.

We are hardly ever able to ascertain the identity of the actor, but one case this quarter does of course stand out: 'attack-g0118', or 'UNC2452' is a suspected Russian state-sponsored threat group believed to be responsible for the 2020 SolarWinds software supply chain intrusion. A more detailed description of this group, their record and their methods can be found here: https://attack.mitre.org/groups/G0118/.

Our Recommendations

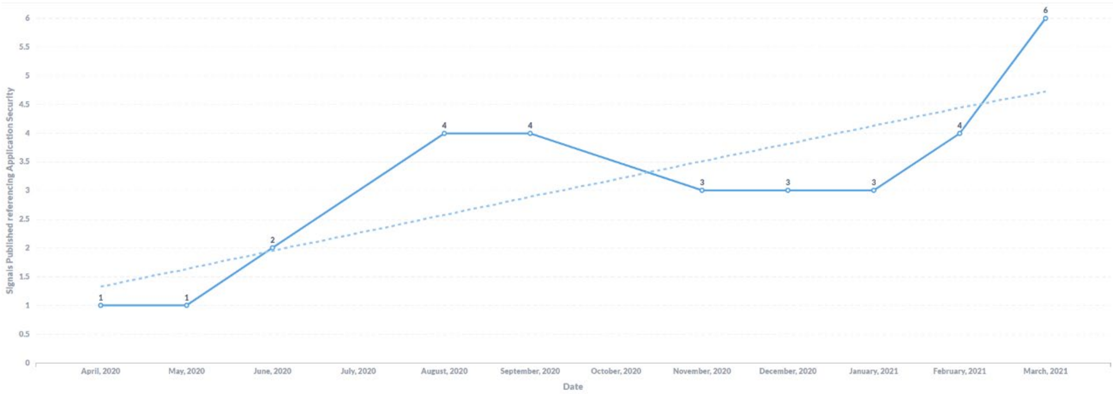
Whenever we include a recommendation in a Signal, that recommendation is mapped to the CIS Top- 20 controls framework (see https://www.cisecurity.org/controls/cis-controls-list/). This allows us to present a view on which standard security controls are occurring most frequently in our advisories



Summary of recommendations made over the last quarter

As has been the clear pattern throughout the year, most of our recommendations fall under the basic CIS controls of Inventory and Vulnerability Management. However, the ranking of these controls has shifted somewhat over time: **Hardware Inventory has become more important** (from 5.9% to 8.3%) and **Account Monitoring & Control** is also featuring much more often (from 3.5% to 6.1%). **Application Software** Security has also climbed the rankings from second lowest to take 7th place in the list of controls we have referenced this quarter. According to the CIS framework, Application Security means to "**manage the security life cycle of all in-house developed and acquired software** in order to prevent, detect, and correct security weaknesses" (https://www.cisecurity.org/controls/application-software-security/).

This increase in the growing relevance of Application Security in our Advisories is very clear to see:



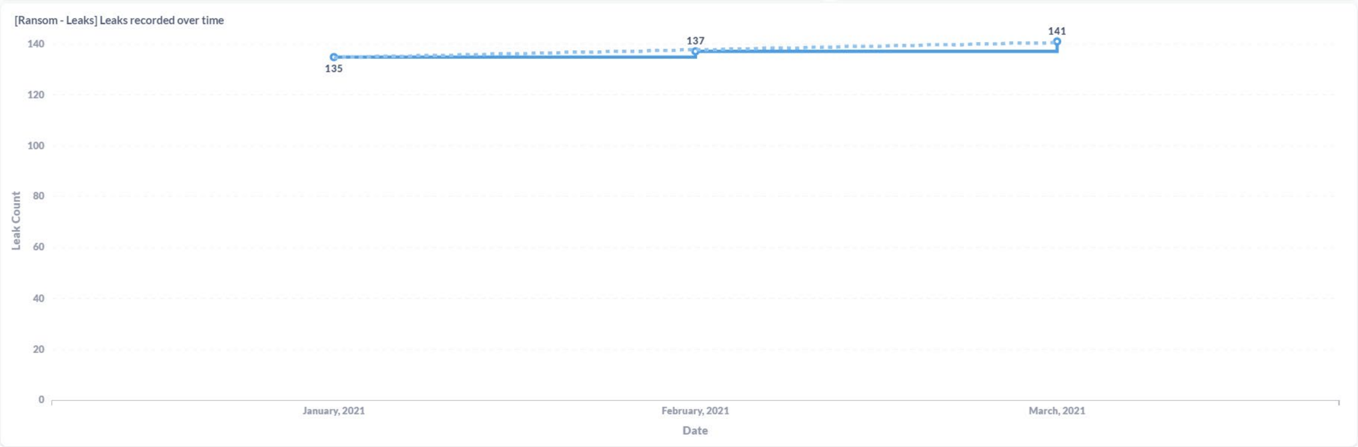
We're talking about Application Security more and more

We haven't referenced Application Security much in our previous reports, so it may be worth reviewing the recent Signals in which this CIS control was sited:

Date	Category	Urgency	Summary
2021/01/06	Breach	Information	Data from August Breach of Amazon Partner Juspay Dumped Online
2021/01/08	Vulnerability	Medium	RCE 'Bug' Found and Disputed in Popular PHP Scripting Framework
2021/01/13	Breach	Information	United Nations data breach exposed over 100k UNEP staff records
2021/02/15	Threat	Medium	Copycat researchers imitate supply chain attack that hit tech giants
2021/02/18	Vulnerability	Low	Security bugs left unpatched in Android app with one billion downloads
2021/02/25	Vulnerability	Medium	Heavily used Node.js package has a code injection vulnerability
2021/02/26	Breach	Information	Health Website Leaks 8 Million COVID-19 Test Results
2021/03/04	News	Medium	Malicious Code Packages Target Amazon, Lyft, Slack, Zillow
2021/03/09	Vulnerability	Information	Newest Intel Side-Channel Attack Sniffs Out Sensitive Data
2021/03/17	Threat	Low	Microsoft's Azure SDK site tricked into listing fake package
2021/03/29	Breach	Information	PHP's Git server hacked to add backdoors to PHP source code
2021/03/30	Breach	Information	MobiKwik Suffers Major Breach
2021/03/31	Advisory	High	Accellion File Transfer Appliance Security Assessment

Ransomware Trends (Beta)

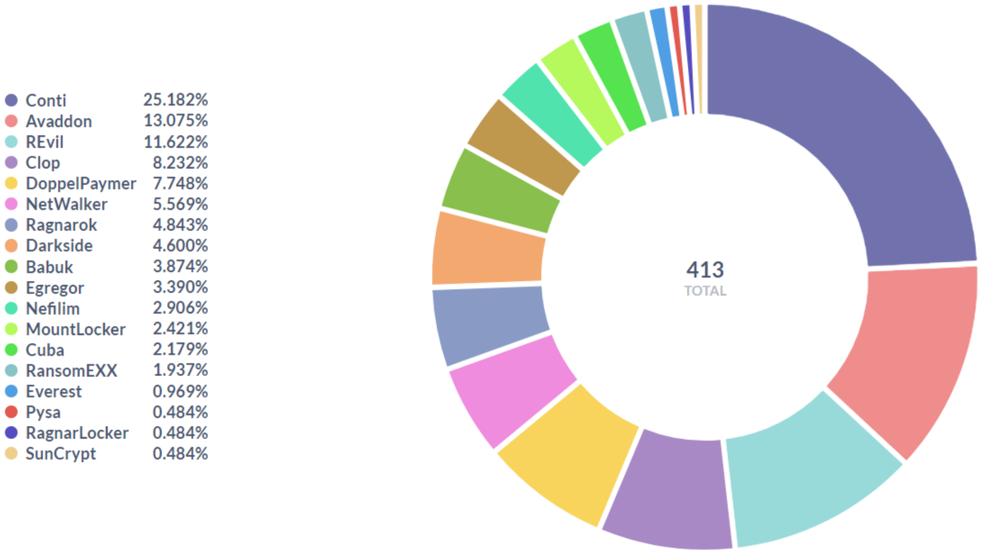
As we previously promised, we have re-implemented our ransomware leak site monitoring program and have succeeded in documenting a set of 413 ransomware leaks since January. We do not yet have sufficient data in through this program to seriously comment on trends over time, but we are able to present some insights based on the data we have.



Total leaks observed over time

The total number of leaks we have been able to observe has grown slightly over the quarter, suggesting that we may have reached a level of 'critical mass' for this kind of operation. However, it's probably too early in this dataset to argue that for certain.

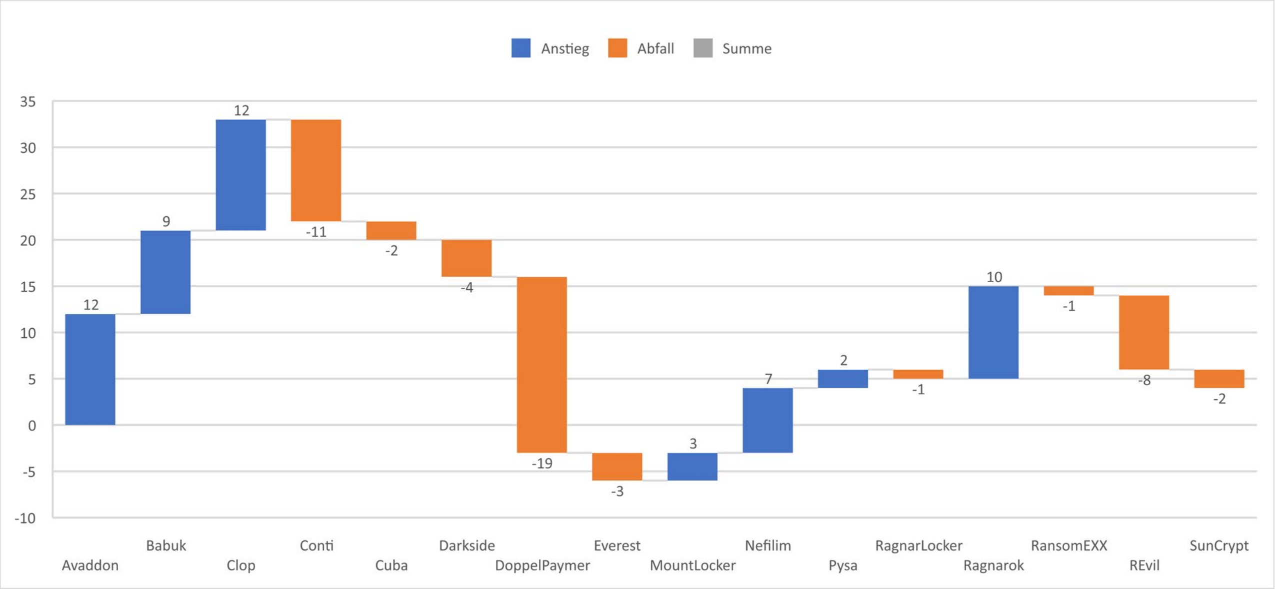
Among the various ransomware crews the level of activity has varied substantially.



Ransomware leaks by Actor – Q1 2021

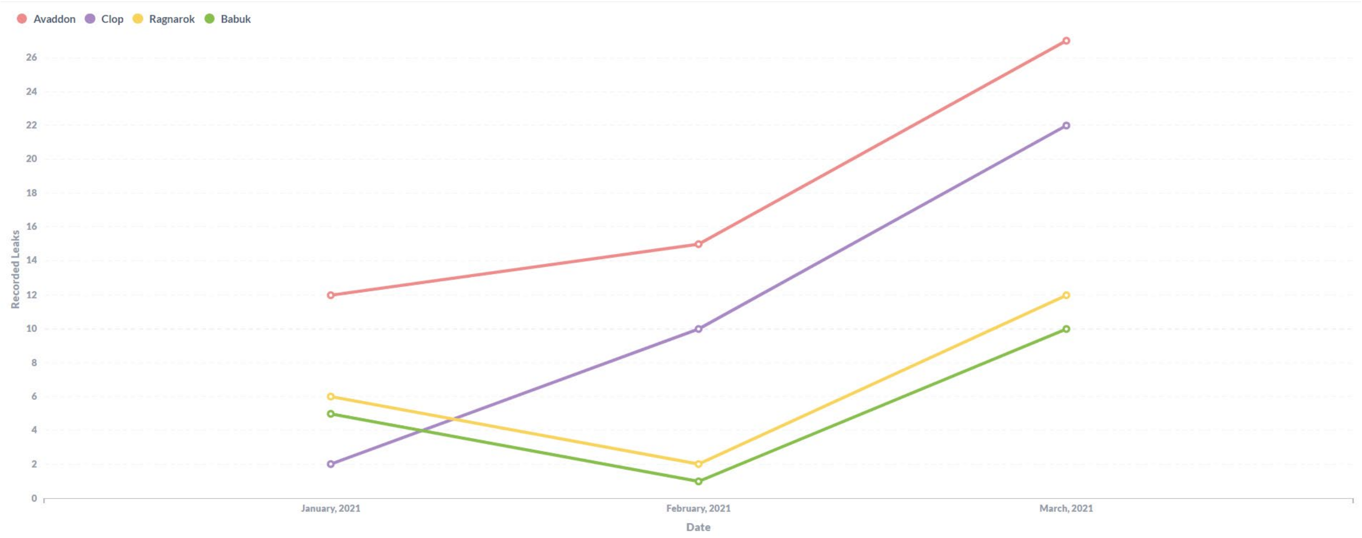
The chart above illustrates that a small number of crews are pulling ahead of the rest of the 'pack' to claim the majority of compromises. Conti, REvil, Cl0p and DoppelPaymer are old hands, but Avaddon is a newer player in the top that is starting to make waves, although they have been active since June 2020.

The most recent activity by these various actors is captured in the chart below:



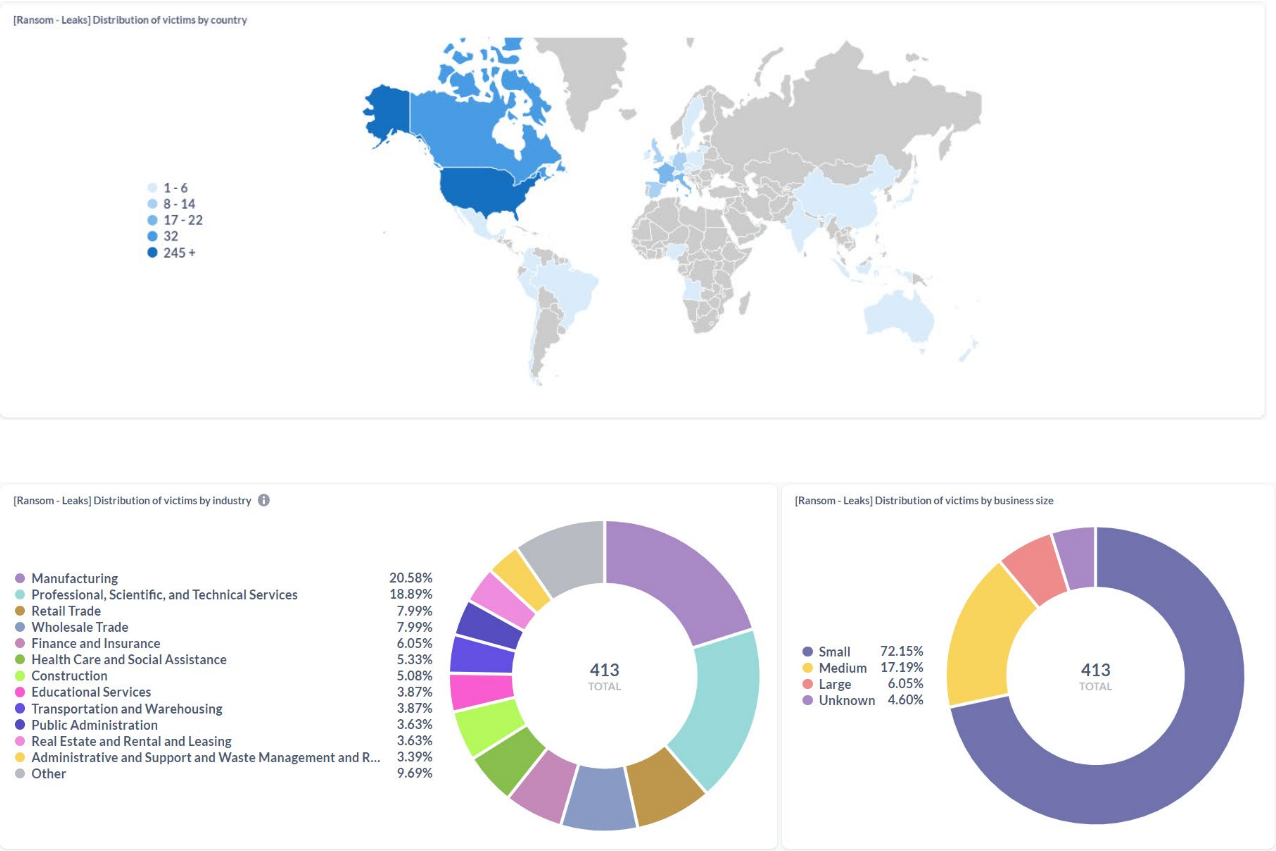
Ransomware actors - changes since February

It’s not clear yet what’s behind the decrease in compromises by the major players – Conti, DoppelPaymer, and REvil- but the significant increase in activity by Avaddon and Babuk is worth noting. Babuk in particular is a recent player that has been making waves:



Avaddon, Babuk, Cl0p & Ragnarok surging

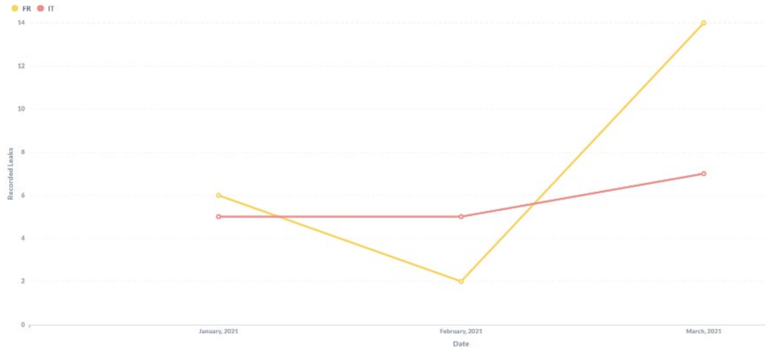
Some familiar trends are also emerging in terms of the victimology:



Recorded leaks distributed across victims

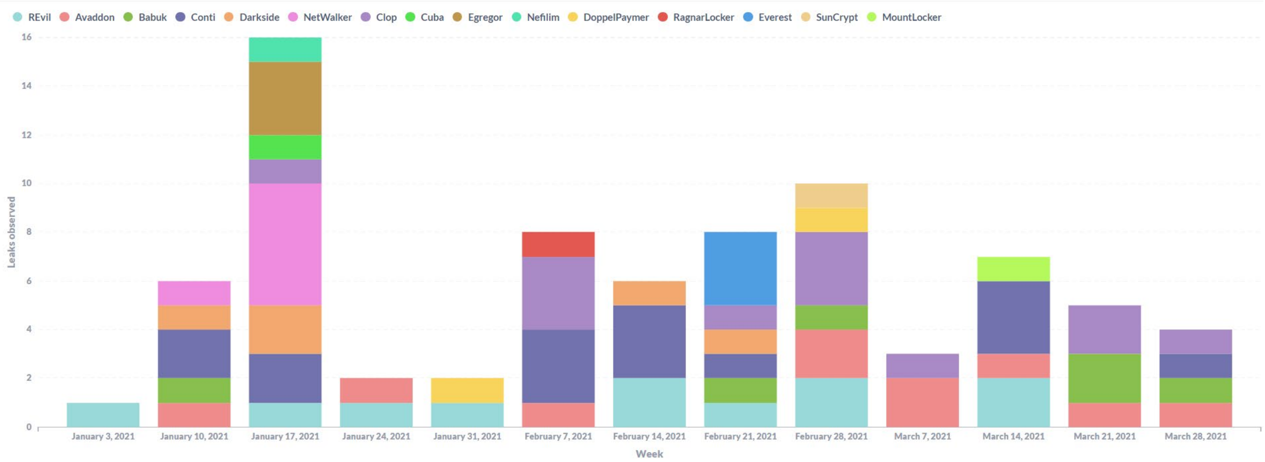
The first thing we notice in an examination of the current set of 413 victims, is the high concentration in the USA. This stands to reason given the vast scale of that geography. Canada is the next most impacted, probably for the same reasons.

The next two most impacted geographies – France and Italy – are interesting, however, as this is not a pattern we have observed before. The volume of incidents impacting Italian businesses has been relatively consistent over time, but **in France we certainly observed a massive spike in compromises during March**. It will be interesting to note whether this trend extends into the future…



In terms of victim industries, it comes as no surprise to see **Manufacturing at the top of the list**, as this echoes the pattern we elsewhere and in previous datasets. The position of '**Professional, Scientific, and Technical Services' in second place comes as somewhat of a surprise** to us.

According to the NAICS the activities performed in this sector include: "legal advice and representation; accounting, bookkeeping, and payroll services; architectural, engineering, and specialized design services; computer services; consulting services; research services; advertising services; photographic services; translation and interpretation services; veterinary services; and other professional, scientific, and technical services”. An examination of leaks impacting this industry shows **a spike of compromises in the middle of January**:



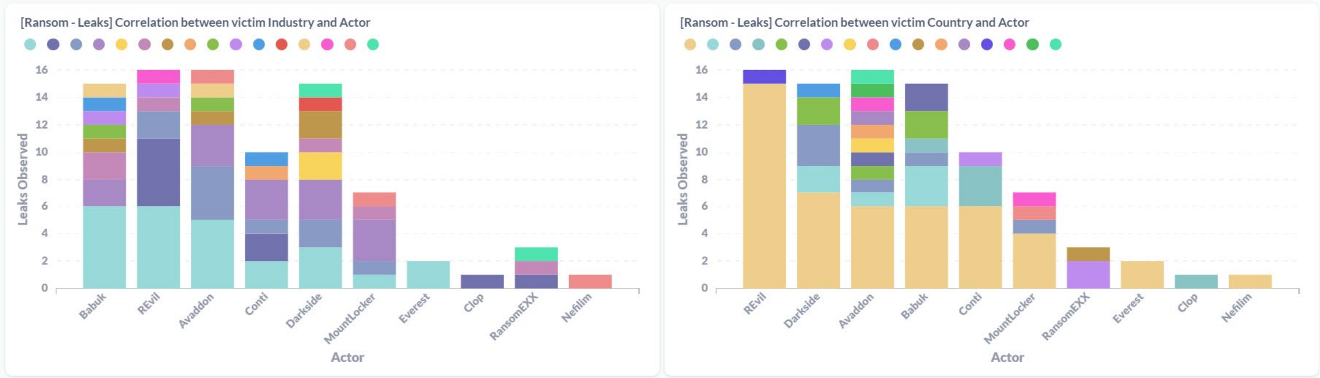
Recorded leaks impacting ‘Professional, Scientific, and Technical Services’

The spike of attacks in January is mostly attributed to Netwalker, who have otherwise been a rather unremarkable mid-tier player. We’ve observed several law firms in this broad industry classification, which may be significant, since for law firms a data breach can mean so much more damage than for others in the same classification. In one case REvil leaks for each (celebrity) client separately on their leaksite.

But a cursory examination of the Netwalker victims shows no other notable similarity, other than that they are classified as ‘Small’ and based in the USA. There don’t seem to be any other strong similarities between the other victims in this sector either, suggesting that **the prominence of the sector is probably not a function of attacker intent as much as some other property of the sector**, like its collective level of security.

A much clearer pattern emerging from an examination of the victims is the **prominence of small business**, with 89% of all victims being classified as either Small (72%) or Medium (17%). Attackers would be interested in maximising revenue, so it seems doubtful that they would be particularly incentivised to target smaller businesses. Rather, our working assumption is that these **smaller businesses are more easily compromised**, and the same is probably true for victims in the Manufacturing and the ‘Professional, Scientific, and Technical Services’ sector.

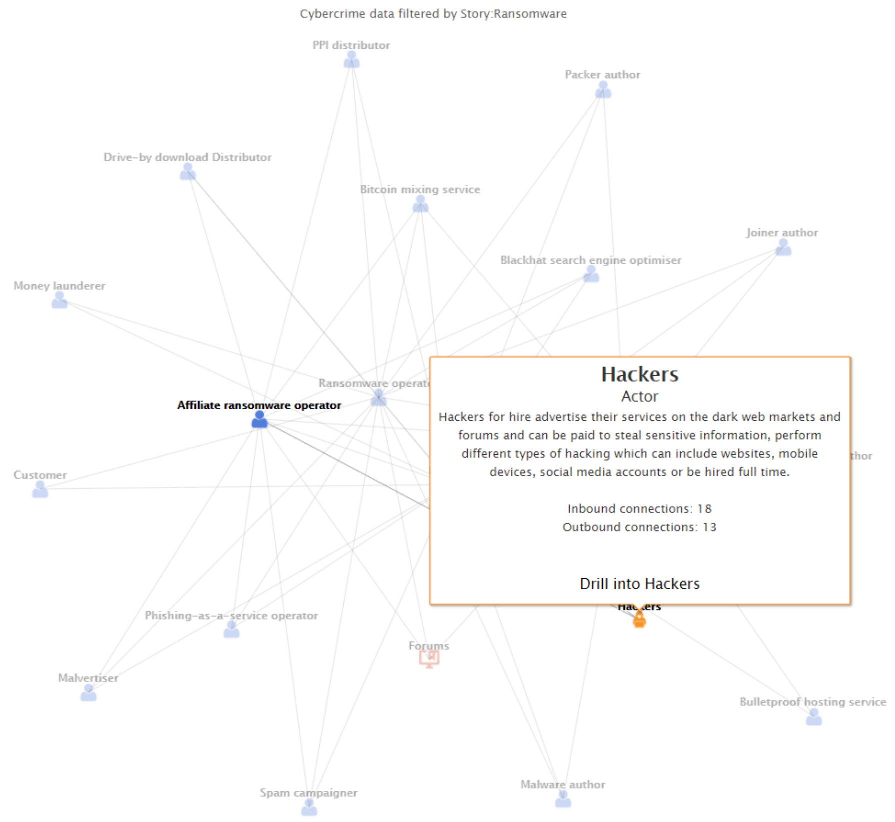
A final visual analysis illustrates this point:



Targeting by ransomware groups Industry and Country

As the chart above appears to illustrate (at least thus far), there is no strong preference by any ransomware operator for a specific industry or country, suggesting that there is no ‘specialisation’ by these groups. Instead, the most frequently hit Industries and Countries are being compromised by all or most of the groups, probably because they offer the best balance between cost of compromise and reward.

Ransomware crews are believed to buy compromised networks from ‘Initial Access Brokers’ (IAB) that sell access based on size and value.


Cybercrime data filtered by Story:Ransomware
PPI distributor
Packer author
Drive-by download Distributor
Bitcoin mixing service
Joiner author
Blackhat search engine optimiser
Money launderer
Ransomware operat
Affiliate ransomware operator
Customer
thor
Phishing-as-a-service operator
Forums
Hac ers
Malvertiser
Bulletproof hosting service
Spam campaigner
Malware author

Hackers
Actor
Hackers for hire advertise their services on the dark web markets and forums and can be paid to steal sensitive information, perform different types of hacking which can include websites, mobile devices, social media accounts or be hired full time.

Inbound connections: 18
Outbound connections: 13

Drill into Hackers

Ransomware operators buy compromises from specialist providers

Somewhere in this market dynamic we imagine the balance between the cost of buying a comprised network from the IAB, and the potential reward of exploiting that compromise for a ransomware, will be struck. It’s this ROI aspect of the market that will determine the victimology. But the starting point is always going to be the availability of the compromised network for purchase from the IAB. Thus, weak security will trump good ROI every time.

Topics (Beta)

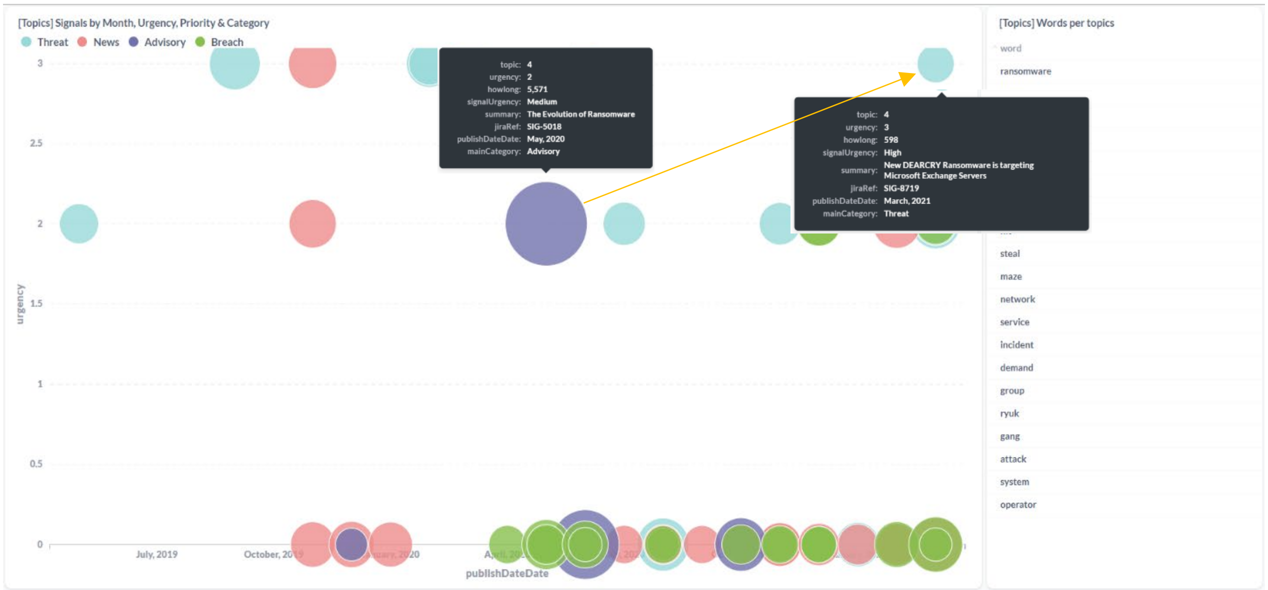
We are experimenting with the use of a Machine Learning approach called ‘Topic Modeling’ to help us glean insight into significant trends and patterns. This is an ongoing development and it’s not clear yet what role this capability will play in our analysis, but in the meantime, we’re excited enough about the technology to share some early findings here:

The topic modeling algorithm looks for sets of matching words and phrases across all our Signals and then groups the Signals together according to ‘topics’. The algorithm doesn’t know what the ‘topics’ refer to, only that the Signals grouped by those topics use similar language. As the chart below illustrates, the algorithm produces fifty distinct topics, consisting of a varying number of Signals from across all our categories.

Given our focus on MS Exchange this month, we focus in the section on a topic that binds the Exchange vulnerability to the broader theme of ransomware and double extortion attacks, specifically through these to recent Signals:

- New DEARCRY Ransomware is targeting Microsoft Exchange Servers
- Microsoft Exchange servers now targeted by BlackKingdom ransomware

Although the MS Exchange vulnerabilities and initial exploits have been loosely attributed to state-backed hackers, ransomware operators have been quick to jump on the train.



topic: 4
urgency: 2
howlong: 5,571
signalUrgency: Medium
summary: The Evolution of Ransomware
jiraRef: SIG-5018
publishDateDate: May, 2020
mainCategory: Advisory

topic: 4
urgency: 3
howlong: 598
signalUrgency: High
summary: New DEARCRY Ransomware is targeting Microsoft Exchange Servers
jiraRef: SIG-8719
publishDateDate: March, 2021
mainCategory: Threat

word
ransomware
steal
maze
network
service
incident
demand
group
ryuk
gang
attack
system
operator

Double extortion as a topic across all our Signals

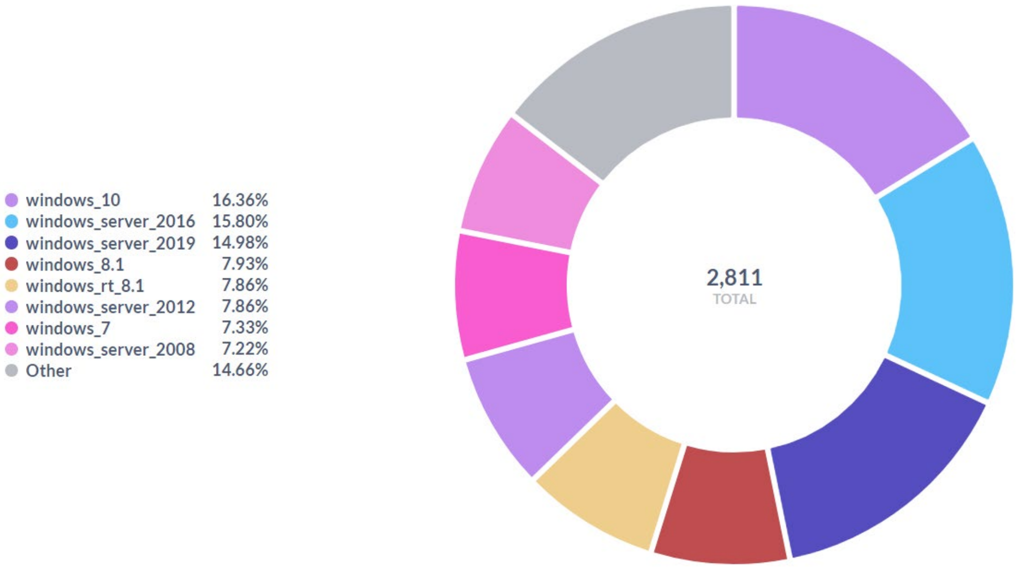
This topic, as is illustrated in the wordlist above, involves ransomware and extortion. The theme emerges most regularly as the low-priority Breach reports that are reflected along the bottom of the chart. There have been more serious threat reports also, however, most notably the report we did of DEARCRY Ransomware targeting Microsoft Exchange.

We took the liberty of highlighting the advisory we published on the issue of double-extortion in May of 2020 and juxtaposing it against the DEARCRY advisory from March, to provide a visual impression of just how much has happened under this heading in those few short months. Sadly, we have every reason to believe this picture will look even worse in another 6 months.

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.

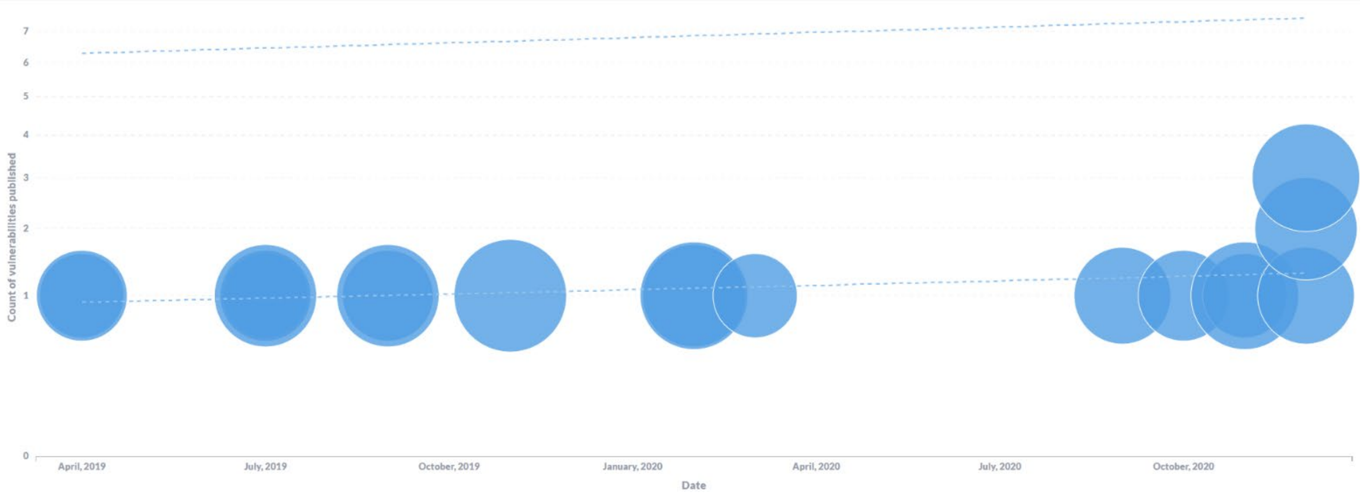
Given the impact of actively exploited Exchange zero-day bugs, we thought that a brief examination of Microsoft vulnerabilities might be in order this month.



High and Critical Vulnerabilities in Microsoft technologies over the last 12 months

Relative to other products in the Microsoft suite, **vulnerabilities in Exchange are relatively uncommon**. The graph above show the distribution of CVEs with a score of 7 or above over the last 12 months. Over 80% of these serious issues fell to the 8 Windows platforms depicted there.

Exchange matches MS Word with 8 serious vulnerabilities in that period and falls in about the middle of the Microsoft products list for vulnerabilities count.

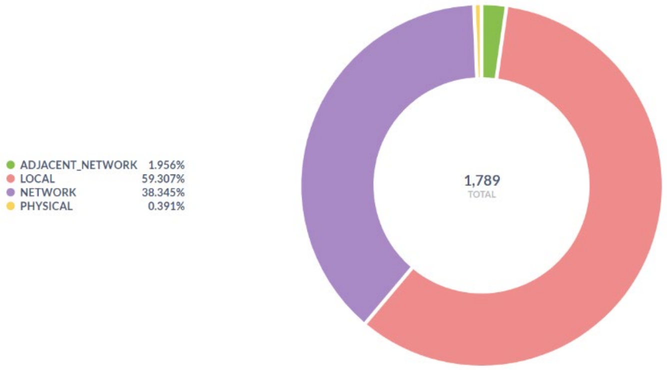


Vulnerabilities in Exchange, showing date, volume, and severity

Exchange has historically had a very good vulnerability track record, but there has been an acceleration of issues with that product in recent months, as the chart above illustrates. The X-axis on the graph shows time, for the last two years. The Y-axis reflects the number of vulnerabilities reported while the size of the bubble reflects the severity. After a distinctly quiet period for Exchange bugs there has been a dramatic increase in both the volume and severity of issues since September 2020.

Volumes aside, Exchange vulnerabilities have another important characteristic, namely that they are often exploitable over the network and often even exposed directly to the Internet.

The chart to the right shows the general exploitability of Windows vulnerabilities for all CVEs over the past two years. In general, almost 60% of Microsoft vulnerabilities require host access to exploit. **For Exchange by contrast, 100% of vulnerabilities recorded over the last 2 years were exploitable over the network**. This stands to reason given the nature of exchange, but also serves as a good reminder of why vulnerability management and patching of Exchange needs to remain a key priority for business that are choosing to run this platform in their own environments.



DATA BREACHES

The threat posed by ransomware is not subsiding and the groups behind these operations are becoming more brazen and successful. They are targeting corporations and governments alike. We have seen ransomware groups like Clop extorting victims of pure data breaches, even though no data was encrypted. This is on the back of a series of breaches involving successful exploitation of Accellion File Transfer Appliances (FTA).

More news about the impact of the SolarWinds supply chain compromise is reaching us. This month Mimecast reported that attackers linked to the supply chain compromise accessed some of its source code, but no code modifications were detected.

High profile data breaches because of the Microsoft Exchange vulnerability known as ProxyLogon have already surfaced. One of the first being the Government of Norway reporting that its parliament’s Exchange server was breached.

Data breaches due to misconfiguration and human error are still making the news. We have also seen how poorly some businesses handle such incidents, causing more drama and fuss than necessary.

Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance

Date: 02 March 2021

A hacking group called 'Hotarus Corp' has hacked Ecuador's Ministry of Finance and the country's largest bank, Banco Pichincha, where they claim to have stolen internal data.

Cybersecurity firm Qualys likely latest victim of Accellion hacks

Date: 04 March 2021

Cybersecurity firm Qualys is the latest victim to have suffered a data breach after a zero-day vulnerability in their Accellion FTA server was exploited to steal hosted files.

SITA data breach affects millions of travellers from major airlines

Date: 08 March 2021

Passenger data from multiple airlines around the world has been compromised after hackers breached servers belonging to SITA, a global information technology company.

Norway parliament data stolen in Microsoft Exchange attack

Date: 11 March 2021

Norway's parliament, the Storting, has suffered another cyberattack after threat actors stole data using the recently disclosed Microsoft Exchange vulnerabilities.

Hacker dumps Guns.com database with customers, admin data

Date: 16 March 2021

The database of Guns.com, a Minnesota US-based platform for selling and buying firearms on-line, was dumped on a hacker forum on March 9, 2021.

Mimecast: SolarWinds Attackers Stole Source Code

Date: 18 March 2021

A new Mimecast update reveals that attckers used the SolarWinds supply-chain compromise to access a "limited" number of source code repositories.

Acer reportedly targeted with $50 million ransomware attack

Date: 22 March 2021

The REvil ransomware gang over the weekend published various Acer documents, such as financial spreadsheets, bank balances, and bank communications.

Energy giant Shell discloses data breach after Accellion hack

Date: 23 March 2021

Energy giant Shell has disclosed a data breach after attackers compromised the company's secure file-sharing system powered by Accellion's File Transfer Appliance (FTA).

Ransomware attack shuts down Sierra Wireless IoT maker

Date: 24 March 2021

Sierra Wireless, a world-leading IoT solutions provider, today disclosed a ransomware attack that forced it to halt production at all manufacturing sites.

CNA insurance firm hit by a cyberattack, operations impacted

Date: 25 March 2021

CNA Financial, a leading US-based insurance company, has suffered a cyberattack impacting its business operations and shutting down its website.

PHP's Git server hacked to add backdoors to PHP source code

Date: 29 March 2021

In the latest software supply chain attack, the official PHP Git repository was hacked and tampered with. Yesterday, two malicious commits were pushed to the php-src Git repository maintained by the PHP team on their servers. The threat actors had signed off on these commits as if they were made by known PHP developers.

FatFace pays out $2 million to Conti ransomware gang

Date: 29 March 2021

UK fashion retailer FatFace, which made headlines this week by appearing to ask its customers to keep its cyber attack “strictly private and confidential”, has reportedly paid a $2 million ransom to the criminals responsible.

Online FX broker FBS leaked 16B customer records via an unsecured server

Date: 30 March 2021

New York-based FBS, a leading foreign exchange broker for online trading, recently left an Elasticsearch server exposed on the Internet that contained over 16 billion data records, including personally identifiable information of its customers.

MobiKwik Suffers Major Breach

Date: 30 March 2021

Popular Indian mobile payments service MobiKwik on Monday came under fire after 8.2 terabytes (TB) of data belonging to millions of its users began circulating on the dark web in the aftermath of a major data breach that came to light earlier this month.

MALWARE AND EXPLOITS

Ransomware operators are constantly evolving their techniques and tactics. This arms race has existed between malware authors and security companies for decades and it is expected to escalate.

We reported on dependency confusion type attacks against prominent software development libraries. This type of attack, if successful, will result in malicious code being pulled into legitimate software development pipelines by accident. Developers need to respond by explicitly qualifying all direct and transitive dependencies.

We saw several exploits involving zero-days targeting browsers and mobile applications. This included a rare glimpse into a western counterintelligence operation that was disrupted by Google's security teams. Normally we cover stories involving Russian, middle eastern, or far east state-affiliated operations, but this somewhat balances a biased news cycle.

IOT devices are increasingly being targeted by botnets. Network Attached Storage devices and home routers are popular targets as these are exposed to the Internet and represents an easy target due to poor configuration and lack of maintenance.

Ryuk ransomware now self-spreads to other Windows LAN devices

Date: 01 March 2021

A new Ryuk ransomware variant with worm-like capabilities that allow it to spread to other devices on victims' local networks has been discovered by the French national cyber-security agency while investigating an attack in early 2021.

Working Windows and Linux Spectre exploits found on VirusTotal

Date: 02 March 2021

Working exploits targeting Linux and Windows systems not patched against a three-year-old vulnerability dubbed Spectre were found by security researcher Julien Voisin on VirusTotal.

Malicious Code Packages Target Amazon, Lyft, Slack, Zillow

Date: 04 March 2021

Attackers have weaponised code dependency confusion to target internal apps at tech giants Amazon, Lyft, Slack and Zillow and more. Researchers uncovered the malicious packages targeting a variety of companies inside the npm public code repository — all of which exfiltrate sensitive information.

Microsoft, FireEye Unmask More Malware Linked to SolarWinds Attackers

Date: 09 March 2021

Researchers with Microsoft and FireEye found three new malware families, which they said are used by the threat group behind the SolarWinds attack.

Hackers hiding Supernova malware in SolarWinds Orion linked to China

Date: 09 March 2021

Intrusion activity related to the Supernova malware planted on compromised SolarWinds Orion installations exposed on the public internet points to an espionage threat actor based in China.

Unpatched QNAP devices are being hacked to mine cryptocurrency

Date: 10 March 2021

Unpatched network-attached storage (NAS) devices are targeted in ongoing attacks where the attackers try to take them over and install cryptominer malware to mine for cryptocurrency.

IoT Devices Under Attack By Tor-Based Gafgyt Variant

Date: 10 March 2021

A new variant of the Gafgyt botnet - that's actively targeting vulnerable D-Link and Internet of Things devices - is the first variant of the malware to rely on Tor communications, researchers say.

New DEARCRY Ransomware is targeting Microsoft Exchange Servers

Date: 12 March 2021

Threat actors are now installing a new ransomware called 'DEARCRY' after hacking into Microsoft Exchange servers using the recently disclosed ProxyLogon vulnerabilities.

Google Releases Spectre PoC Exploit For Chrome

Date: 16 March 2021

Google has released the side-channel proof-of-concept (PoC) exploit code, which leverages the Spectre attack against the Chrome browser to leak data from websites, in hopes of motivating web-application developers to protect their sites.

FBI warns of escalating Pysa ransomware attacks on education orgs

Date: 17 March 2021

The Federal Bureau of Investigation (FBI) Cyber Division has warned system administrators and cybersecurity professionals of increased Pysa ransomware activity targeting educational institutions in 12 US states and the United Kingdom.

Latest Mirai Variant Targets SonicWall, D-Link and IoT Devices

Date: 17 March 2021

A new Mirai variant is targeting known flaws in D-Link, Netgear and SonicWall devices, as well as newly-discovered flaws in unknown IoT devices.

Microsoft's Azure SDK site tricked into listing fake package

Date: 17 March 2021

A security researcher was able to add a counterfeit test package to the official list of Microsoft Azure SDK latest releases. The simple trick if abused by an attacker can give off the impression that their malicious package is part of the Azure SDK suite.

Chinese APT group targets telcos in 5G-related cyber-espionage campaign

Date: 17 March 2021

A major espionage campaign dubbed Operation Diànxùn is targeting major telecommunications companies in Europe, US and Southeast Asia.

New APT group SilverFish Has Compromised Thousands of Victims

Date: 19 March 2021

A threat actor dubbed SilverFish is responsible for intrusions in 4,720 organisations and uses the compromised systems as playgrounds to test out malicious tool detection rates.

FBI: Phishing emails are spreading this sophisticated malware

Date: 22 March 2021

Alert by the FBI and CISA warns that Trickbot - one of the most common and most powerful forms of malware around - is using a new trick in an effort to infect even more victims.

Hacking group used 11 zero-days to attack Windows, iOS, Android users

Date: 30 March 2021

Project Zero, Google's zero-day bug-hunting team, discovered a group of hackers that used 11 zero-days in attacks targeting Windows, iOS, and Android users within a single year. The Project Zero team revealed that the hacking group behind these attacks ran two separate campaigns, in February and October 2020.

Hades ransomware targets big firms

Date: 30 March 2021

Major cybersecurity companies such as Crowdstrike, Accenture and Awake security have published different analysis of the Hades ransomware.

VULNERABILITY MANAGEMENT

This month we learned of a set of vulnerabilities referred to as ProxyLogon. These vulnerabilities in Microsoft Exchange resulted in a patch frenzy as system administrators rushed to protect their systems after it was revealed how easy these vulnerabilities are to exploit. Attackers have already had great success with this and several breaches were reported on the back of this.

A serious F5 BIG-IP vulnerability was also reported this month and some IT teams had a hard time balancing patching priority as they had to manage the fallout resulting from the ProxyLogon vulnerabilities.

This month we learned how attackers exploited Accellion FTA. Accellion released a report that was prepared by Mandiant. In the report we saw that attackers crafted exploits to target 4 zero-day vulnerabilities. These led to several large businesses reporting data breaches.

VMware also had a busy month, releasing security fixes for two vulnerabilities that could be exploited remotely without credentials.

Google and Apple released a slew of security fixes for zero-day vulnerabilities in Chrome and Safari browsers respectively. Some of these are known to be linked with state-affiliated campaigns.

Several Industrial Control System vendors released updates to address vulnerabilities in their products. We have seen some big names in this space coming under pressure to respond quickly because of security researchers finding flaws stretching back years.

Rockwell Automation vulnerability

Date: 03 March 2021

A critical security vulnerability in widely deployed industrial software produced by Rockwell Automation lets a remote attacker connect to almost any of the company’s Logix programmable logic controllers (PLCs).

Microsoft fixes actively exploited Exchange zero-day bugs, patch now

Date: 03 March 2021

Microsoft has released emergency out-of-band security updates for all supported Microsoft Exchange versions that fix four zero-day vulnerabilities actively exploited in targeted attacks.

Google fixes second actively exploited Chrome zero-day bug this year

Date: 04 March 2021

Google has fixed an actively exploited zero-day vulnerability in the Chrome 89.0.4389.72 version released today, March 2nd, 2021, to the Stable desktop channel for Windows, Mac, and Linux users.

GRUB2 boot loader reveals multiple high severity vulnerabilities

Date: 04 March 2021

GRUB, a popular Linux boot loader project has fixed multiple high severity vulnerabilities.

Windows DNS SIGRed bug gets first public RCE PoC exploit

Date: 05 March 2021

A working proof-of-concept (PoC) exploit is now publicly available for the critical SIGRed Windows DNS Server remote code execution (RCE) vulnerability.

VMware releases fix for severe View Planner RCE vulnerability

Date: 05 March 2021

VMware has addressed a high severity unauth RCE vulnerability in VMware View Planner, allowing attackers to abuse servers running unpatched software for remote code execution.

Security Patch for Apple Safari Browser

Date: 09 March 2021

Apple has released out-of-band patches for iOS, macOS, watchOS, and Safari web browser to address a security flaw that could allow attackers to run arbitrary code on devices via malicious web content.

Newest Intel Side-Channel Attack Sniffs Out Sensitive Data

Date: 09 March 2021

A new side-channel attack takes aim at Intel's CPU ring interconnect in order to glean sensitive data.

Microsoft Patch Tuesday Updates Fix 14 Critical Bugs

Date: 10 March 2021

Microsoft's regularly scheduled March Patch Tuesday updates address 89 CVEs overall.

F5 urges customers to patch critical BIG-IP pre-auth RCE bug

Date: 11 March 2021

F5 Networks, a leading provider of enterprise networking gear, has announced four critical remote code execution (RCE) vulnerabilities affecting most BIG-IP and BIG-IQ software versions.

Netgear fixes 15 vulnerabilities in SOHO switch

Date: 12 March 2021

Netgear has released a swathe of security and firmware updates for its JGS516PE Ethernet switch after researchers from NCC Group discovered 15 vulnerabilities in the device – including an unauthenticated remote code execution flaw.

Vulnerabilities Found in Schneider Electric Power Meters

Date: 12 March 2021

Industrial cybersecurity firm Claroty this week disclosed technical details for two potentially serious vulnerabilities affecting PowerLogic smart meters made by Schneider Electric.

SAP Patches Critical RCE Flaw in Manufacturing Software and More

Date: 15 March 2021

The critical bug fixes were part of 18 security patches released by SAP this month. The remote code execution flaw could allow attackers to deploy malware, modify network configurations and view databases.

Google Warns Mac, Windows Users of Chrome Zero-Day Flaw

Date: 16 March 2021

Google is hurrying out a fix for a vulnerability in its Chrome browser that's under active attack – its third zero-day flaw so far this year.

Cisco Plugs Security Hole in Small Business Routers

Date: 18 March 2021

The Cisco security vulnerability exists in the RV132W ADSL2+ Wireless-N VPN Routers and RV134W VDSL2 Wireless-AC VPN Routers.

GitLab Security Release

Date: 19 March 2021

GitLab recently released patches for vulnerabilities, including a remote code execution bug, in dedicated security releases.

Two (unconfirmed) critical zero-day flaws in Microsoft Office 365

Date: 19 March 2021

A cybersecurity researcher called Chetan Nayak (or "Paranoid Ninja" on Twitter) reported to Microsoft two allegedly critical zero-day vulnerabilities in Microsoft Office365 that could allow attackers to completely bypass the authentication process on the target system.

Microsoft Exchange servers now targeted by BlackKingdom ransomware

Date: 23 March 2021

Another ransomware operation known as 'BlackKingdom' is exploiting the Microsoft Exchange Server ProxyLogon vulnerabilities to encrypt servers.

Critical code execution vulnerability fixed in Adobe ColdFusion

Date: 23 March 2021

Adobe has released out-of-band security updates to address a critical vulnerability impacting ColdFusion versions 2021, 2016, and 2018.

CISA Warns of Security Flaws in GE Power Management Devices

Date: 24 March 2021

The flaws could allow an attacker to access sensitive information, reboot the UR, gain privileged access, or cause a denial-of-service condition.

Cisco addresses critical bug in Windows, macOS Jabber clients

Date: 25 March 2021

Cisco has addressed a critical arbitrary program execution vulnerability impacting several Cisco Jabber client software for Windows, macOS, Android, and iOS.

OpenSSL fixes severe DoS, certificate validation vulnerabilities

Date: 26 March 2021

OpenSSL has patched two high severity vulnerabilities. These include a Denial of Service (DoS) vulnerability (CVE-2021-3449) and an improper CA certificate validation issue (CVE-2021-3450).

Apple fixes iOS zero-day vulnerability exploited in the wild

Date: 29 March 2021

Apple has released security updates today to address an iOS zero-day bug actively exploited in the wild and affecting iPhone, iPad, iPod, and Apple Watch devices.

Thousands of applications impacted by critical vulnerability in netmask library

Date: 31 March 2021

A "critical" vulnerability has been found in popular package called netmask, used by hundreds of thousands of applications. It has over 3 million weekly downloads on the official NPM packages' download site and about 279,000 GitHub repositories depend on it.

A vulnerability allowing an attacker to steal credentials on vRealize fixed by VMware

Date: 31 March 2021

VMware has published security updates to address a high severity vulnerability in vRealize Operations that could allow attackers to steal admin credentials after exploiting vulnerable servers. vRealize Operations is an AI-powered and "self-driving" IT operations management for private, hybrid, and multi-cloud environments, available as an on-premises or SaaS solution.

Accellion File Transfer Appliance Security Assessment

Date: 31 March 2021

Accellion shared details of a security assessment report produced by Mandiant on review of the File Transfer Appliance (FTA) that was widely exploited to steal sensitive information.

NOTEWORTHY

OVH data centre destroyed by fire in Strasbourg

Date: 10 March 2021

In a major unprecedented incident, data centers of OVH located in Strasbourg, France have been destroyed by fire.

Ryuk ransomware hits 700 Spanish government labor agency offices

Date: 12 March 2021

The systems of SEPE, the Spanish government agency for labor, were taken down following a ransomware attack that hit more than 700 agency offices across Spain.

Cyber incident at University of the Highlands and Islands

Date: 12 March 2021

On March 8, 2021 the University of the Highlands and Islands (UHI) in Scotland shut down its campuses in response to its attempt to fend off "an ongoing cyber incident".

PPS hit by cyber attack

Date: 16 March 2021

PPS, a South African insurance and investment advisory company, has suffered a cyber attack at the hands of unknown hackers.

Birmingham College Closed After Cyber Attack

Date: 16 March 2021

The eight sites of South and City College Birmingham will be shut and revert to online teaching from today while computer forensic specialists work to fix the problem.

Sky ECC denies police have ‘cracked’ encrypted messaging platform

Date: 11 March 2021

Europol, however, says arrests have been made based on monitoring conversation flows.

Nifty Gateway Digital Art Marketplace Account Compromise

Date: 19 March 2021

On March 15, 2021 Nifty Gateway, blockchain based collectable digital art marketplace, published a statement via Twitter to address claims by its users that their accounts were compromised and that they had lost digital assets. Nifty Gateway says that compromised accounts lacked MFA protection and had weak passwords. Some Nifty Gateway users claimed that their linked credit cards were used to purchase digital artwork and that digital artwork was transferred or sold without their consent.

Australian TV station Channel 9 misses broadcasts after cyber-attack

Date: 29 March 2021

A mysterious cyber-attack, believed to have been a ransomware infection, has hit Australian TV station Channel 9 over the weekend and prevented the network from airing some of its normal shows on Sunday.

New Allegations of Questionable Data Breach Handling by Ubiquiti

Date: 31 March 2021

Brian Krebs reports on a whistleblower claiming that Ubiquiti Networks did not reveal material important facts of the data breach disclosed on January 11, 2021.