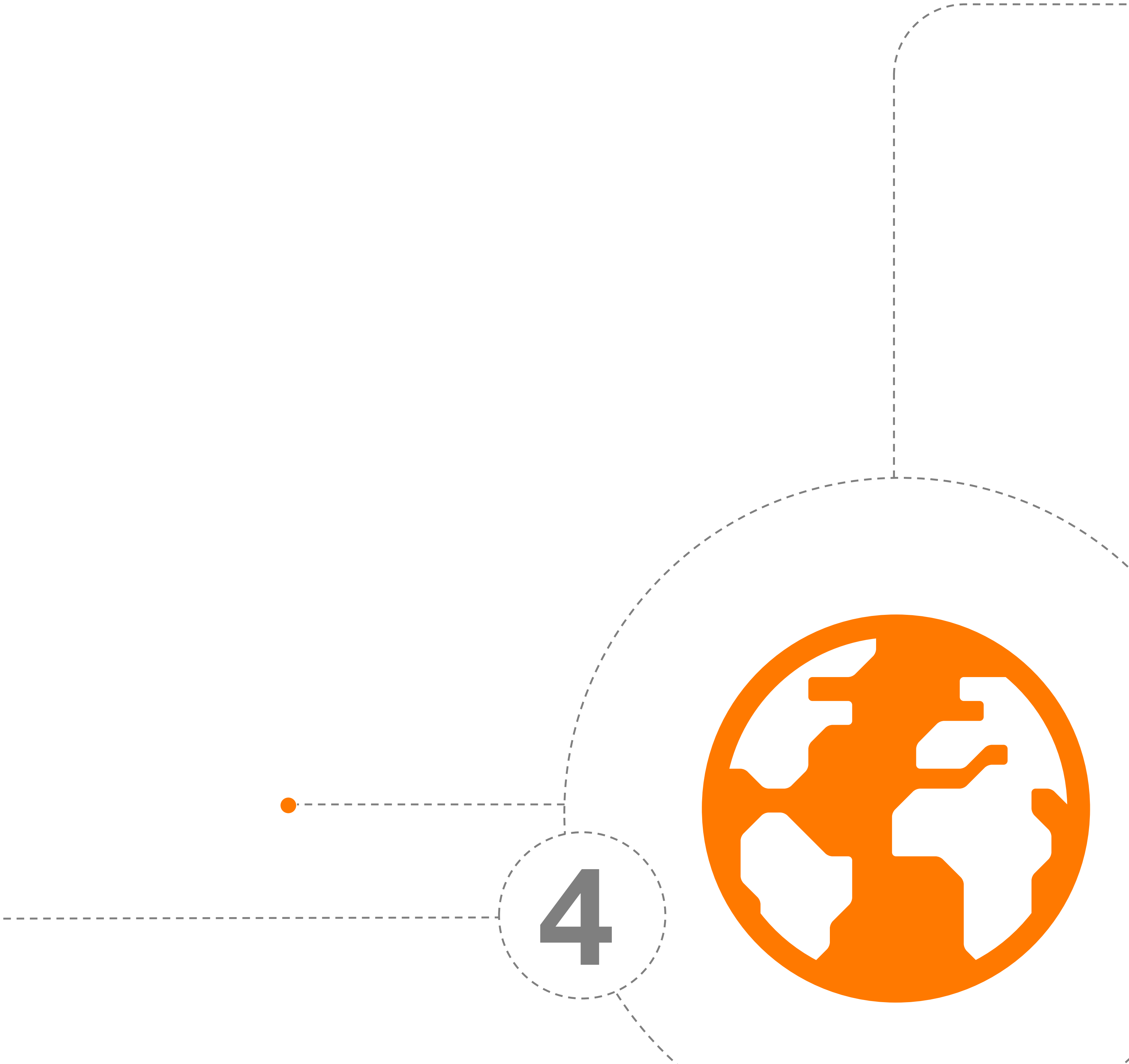
Orange
Cyberdefense

World Watch | Threat Intelligence Report

Monthly Report
April 2021



CONTENTS

INTRODUCTION

This month's report highlights the asymmetry that currently exists between attackers and defenders in cyberspace. It shows that the current reality in cybersecurity favours the attacker and that those tasked with protecting infrastructure and data cannot hope to succeed if we persist with our current practices.

We published 6 Signals that cover zero-days. One of these involves yet another set of zero-day vulnerabilities that Microsoft fixed for Exchange on top of the ones they fixed the prior month.

Apple was not spared from the zero-day frenzy and pushed out fixes for vulnerabilities that could allow an attacker to bypass protections intended to guard against malicious applications executing on a host.

Following that we published a zero-day vulnerability that was reported for Pulse Connect Secure, and it was revealed that this was already being targeted by state-affiliated attackers. Initially only a configuration mitigation was released to guard against potential attack with the prospect of a fix a couple of weeks away.

A security researcher published proof-of-concept exploit code for zero-days targeting the popular Google Chrome and Microsoft Edge browser. Fortunately, the proof-of-concept lacked a complete execution chain that would allow it to escape the Chromium browser sandbox.

SensePost, the ethical hacking team of Orange Cyberdefense, published details on a Duo Two-Factor Authentication bypass they discovered. The flaw could have allowed an attacker to divert the push notification associated with a targeted account to a device under their control instead.

Weaknesses in security products remain a common theme. We published three Signals that relate to attackers exploiting weaknesses in security technologies. Two of these covered ransomware groups that were using weaknesses in Secure Remote Access technologies to breach victims, which is reminiscent of the story we mentioned earlier involving zero-days in Pulse Connect Secure being exploited by state-affiliated attackers. The third Signal that we covered provided details of ongoing exploitation of an anti-malware and anti-spam product originally disclosed in middle 2020.

At a glance

Weaknesses in security products remain a common theme and are frequently targeted by attackers.

We covered two Signals involving supply chain compromise. One incident affected a software development platform that specialise in code testing and verification while another involved a company specialising in password management. The former was breached by exploiting a weakness in an upload script, while the latter exploited a software update mechanism to deliver malicious code to clients.

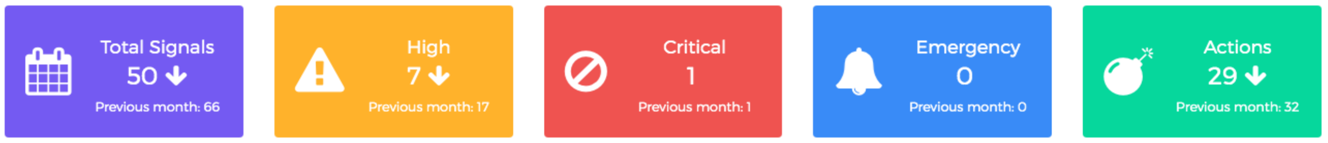
CISA shared details of a breach they investigated that involved a backdoor called Supernova that was injected into a deployed instance of SolarWinds Orion. This incident was not linked to the supply chain compromise reported in December 2020. Attackers breached the perimeter by using a Pulse Connect Secure VPN and weak credentials to simply login like a normal remote user.

We covered three Signals that discussed the evolution of attackers backed by the North Korean government. These Signals highlighted the evolution of the tools and techniques used by these attackers.

OVERVIEW

In this section of the report, we 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
50 ↓
Previous month: 66

High
7 ↓
Previous month: 17

Critical
1
Previous month: 1

Emergency
0
Previous month: 0

Actions
29 ↓
Previous month: 32

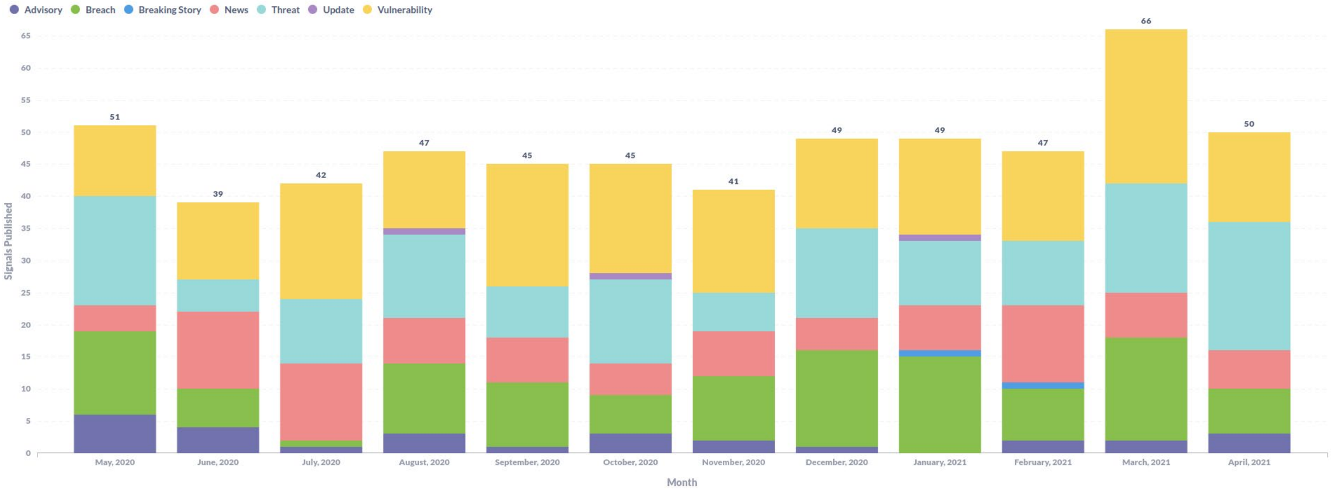
The Signal numbers for April 2021 are down from our previous record month but still higher than our rolling 12-month average of approximately 48 Signals per month. The number of actions we logged with the respective operational teams remains high and we came close to last month's record.

The number of Signals rated 'High' for February and January 2021 are 12 and 13 respectively, making April 2021's number of 7 seem remarkably low.

Our 'Signals' are organised 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

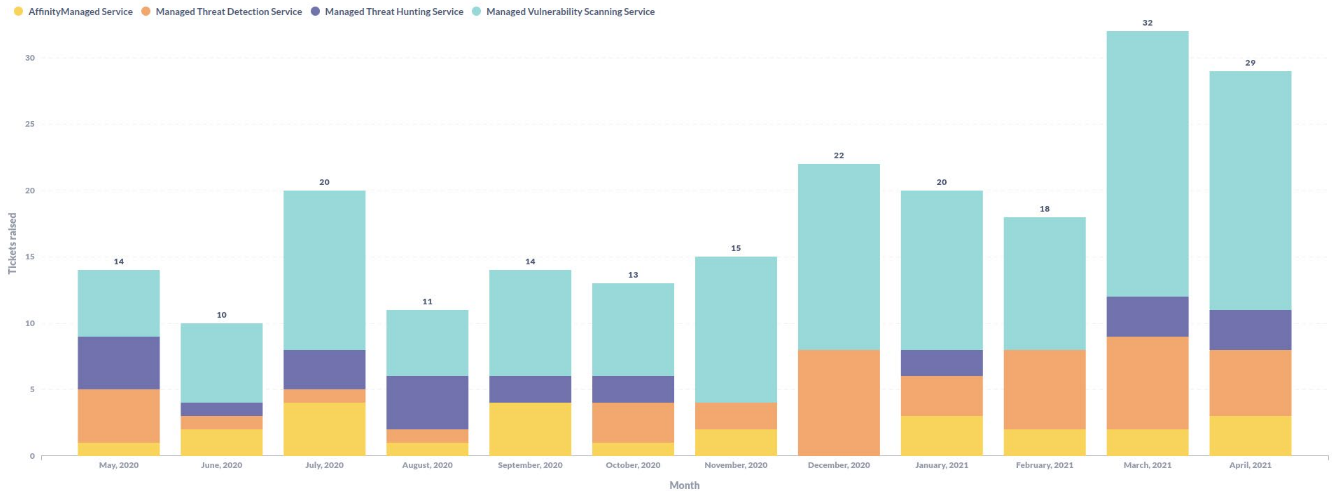


Signals by Category per Month

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

We note that April has been our third busiest month in the last 12 months, with more Threats reported than Vulnerabilities and Breaches.

Services Affected



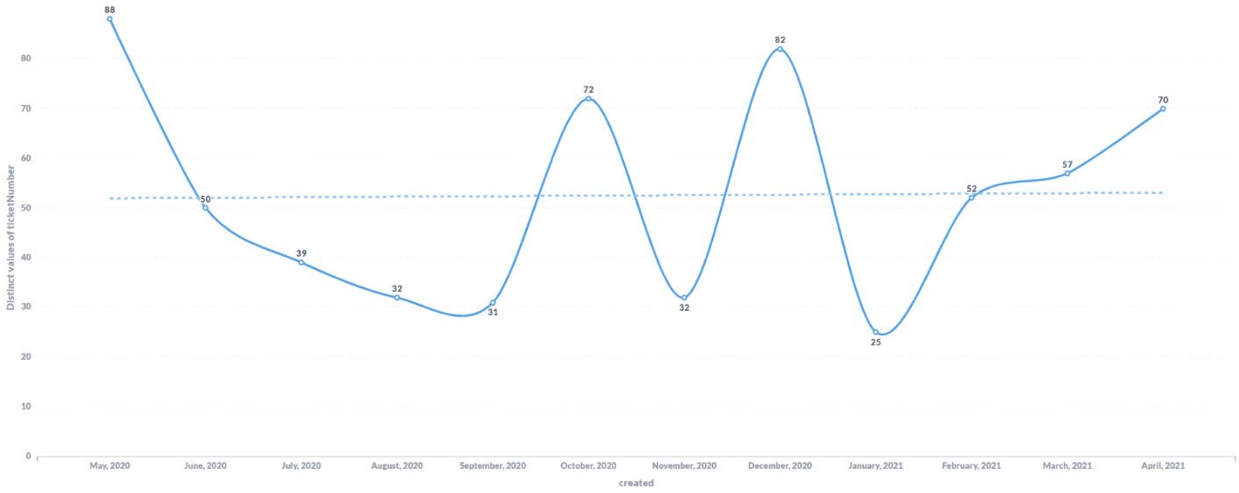
Tickets logged with our operations teams over the last 12 months

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 May 2020 is reflected on the graph above.

Our teams are being kept under continued pressure by the significant volume of vulnerabilities in the security technologies we manage for our customers. The zero-day vulnerability that was reported for Pulse Connect Secure this month, and is already being targeted by state-affiliated attackers, is a prime example of this

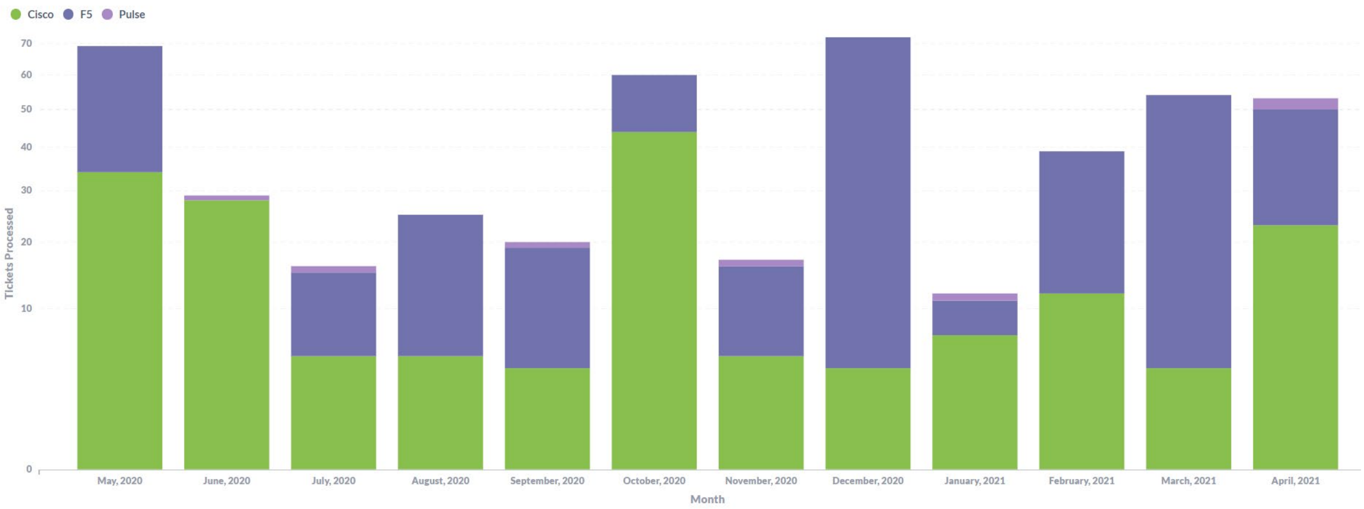
The chart below shows the number of vendor security advisories processed by our UK SOC over the last 12 months.



Vendor Security Advisories processed by our UK SOC

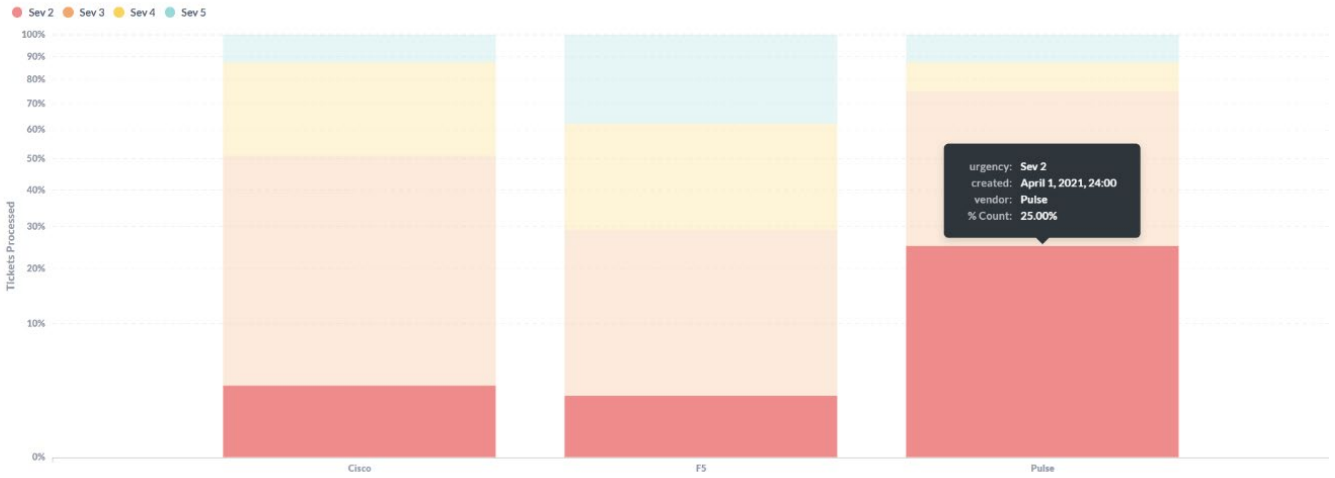
We **note the peak in volume during May last year that occurred during the COVID-19 lockdown** period. This was an extraordinary period, which we have commented on frequently in our 2020 Security Navigator report and elsewhere. The flow of vulnerabilities slowed notably after that, until the **volumes started to increase again in the 4th quarter of 2020.** There was a dip over Christmas, but volumes have grown again to make April the 4th busiest of the last 12 months.

The three Vendor issues noted by the World Watch team this month involved Cisco, F5 and Pulse. We examine the volume and severity of vulnerabilities for these three vendors over time below:



Vendor Security Advisories processed by our UK SOC

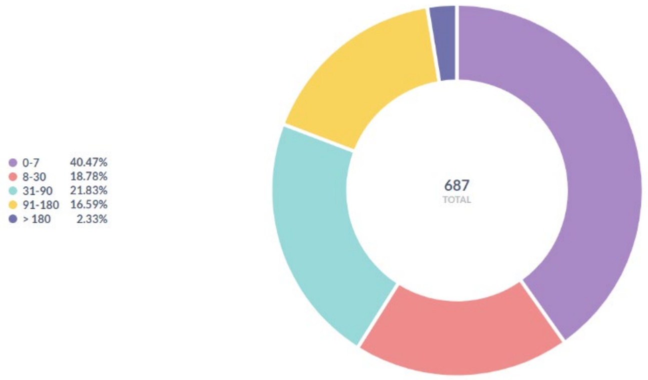
Predictably our SOC needs to process Cisco advisories more than any other, simply due to the sheer volume of products in their stable. F5 also features very frequently, however, despite an arguably smaller portfolio, and release several advisories almost every month. Pulse advisories appear frequently, but not regularly, and in much lower volumes than the other vendors in question. However, an examination of the relative severity of these advisories paints a slightly different picture.



Vendor Security Advisories by Severity

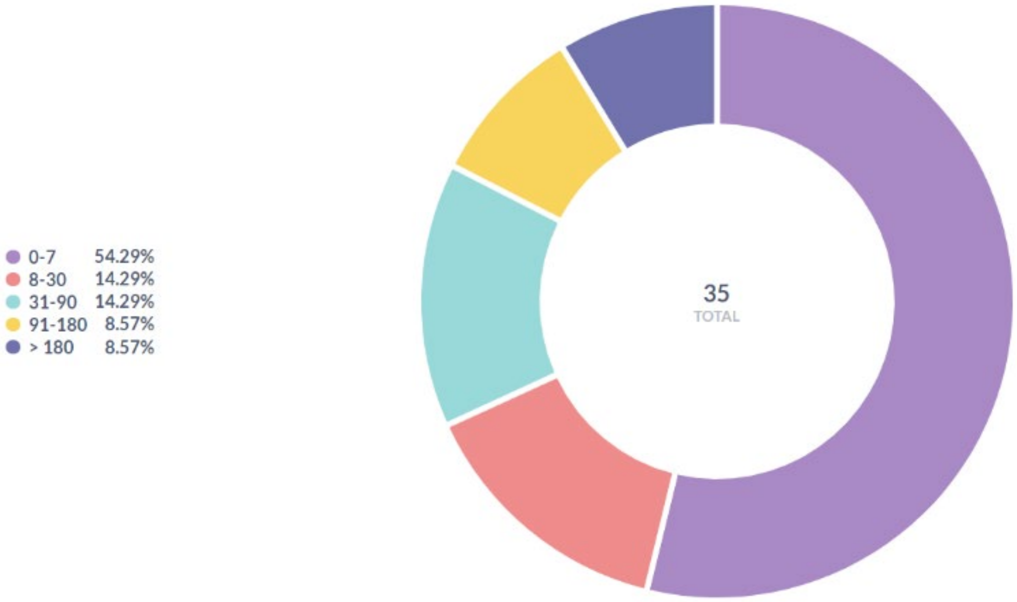
Our UK SOC hasn't processed a vendor security advisory as 'Sev 1' (the highest possible level) in the last 12 months, so 'Sev 2' represents the highest level of urgency in question over that period. In the chart above we look at the percentage distribution of severity levels for the three different vendors.

For Pulse, 6 of the 8 advisories (75%) released by them have been Severity 2 or 3. For Cisco Sev 2 & 3 represent 50% of advisories for F5 it's less than 30%.



The vendor advisories documented are received and processed by our SOC to determine whether they impact our customers. This analysis involves understanding the specific versions and features that are impacted, as well as the attributes required for the proposed remediation. Once they have identified impacted devices, a ticket is logged with the assigned engineer who in turn provides the appropriate guidance to the customer. At this point the ticket raised for the inbound advisory can be closed. The chart to the left illustrates how long it generally takes our SOC analysts to complete this process.

Only a small portion of the advisories we receive evolve into tickets raised with customers. We examined the resolution times of 35 such tickets to determine how long it takes our customers to respond to the security tickets we raise with them.

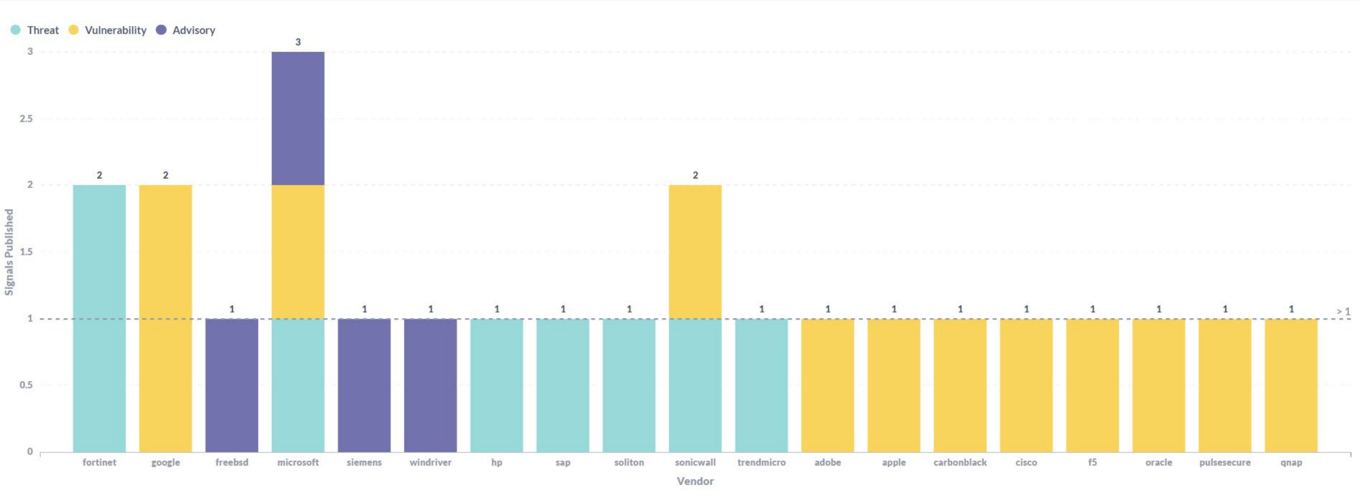


Resolution time windows for security tickets logged with customers

From the data above we note that about 55% of these tickets are resolved with customers within 7 days. About 68% are resolved within a month**. Several advisories still take longer than a month to resolve, however. This is clearly too long.**

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 is contributing in a direct way to compromises and breaches.

Technologies Affected

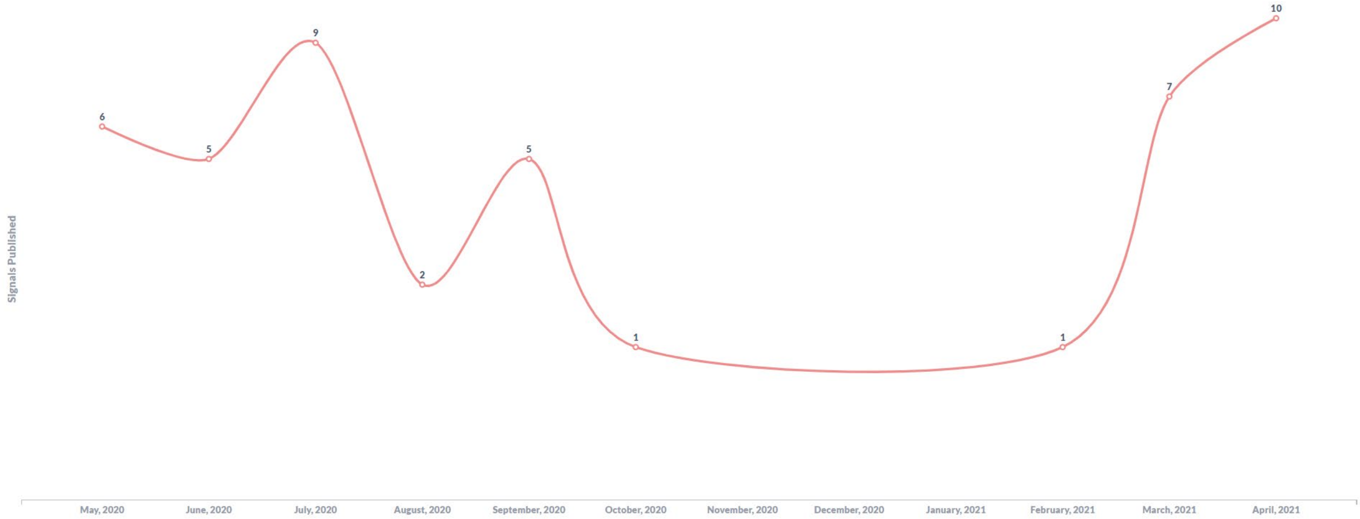


Technologies featuring in our Signals in April

The chart above summarises the technology vendors that were referenced in our Signals during April.

As was the case for last month, two features emerge again from this perspective.

Firstly, we see the growing prevalence of security technologies among the threats and vulnerabilities we must contend with. This is a trend we actively track in our World Watch service data, and we can see that in April this year we hit a new monthly high:



Advisories regarding security technologies peaked in April

In April we specifically tagged several security vendors in advisories, including Fortinet, SonicWall, Trend Micro, Carbon Black, F5 & Pulse Secure.

Notable Advisories regarding security technologies during April include:

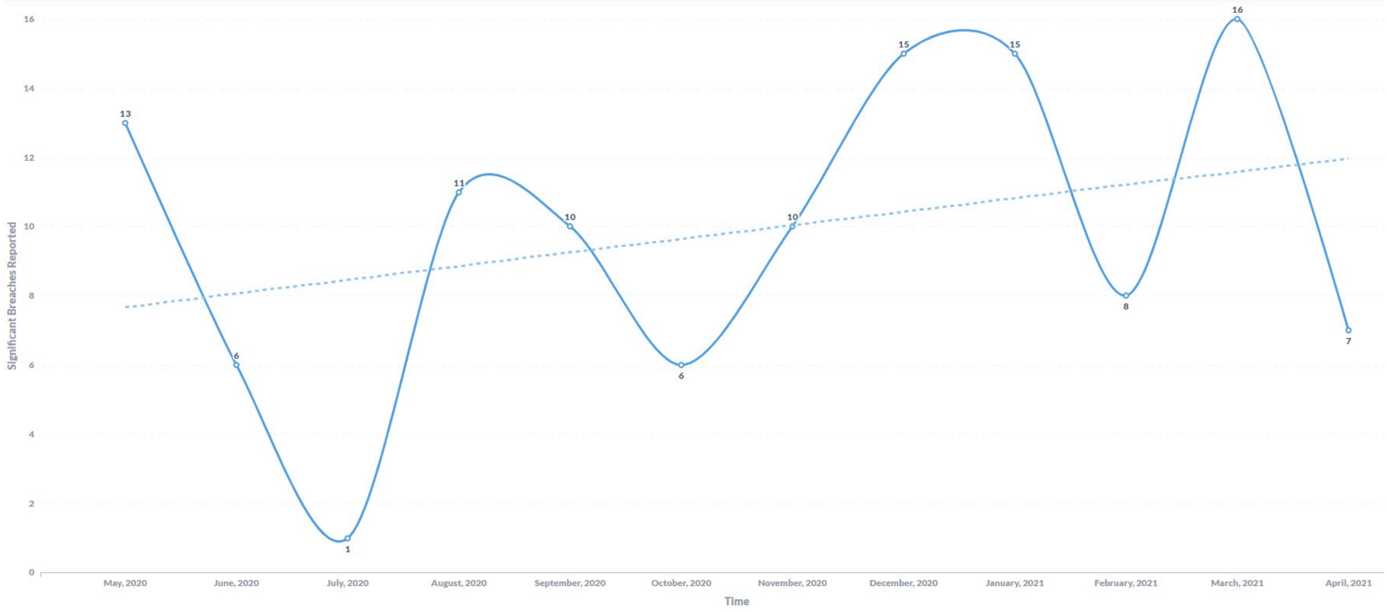
Date	Summary
2021/04/02	Critical vulnerability in the VMware Carbon Black Cloud Workload appliance discovered
2021/04/16	Malicious copycats of Zoom and Windscribe personal VPN used in the wild
2021/04/20	SensePost Discovers Authentication Bypass in Duo 2FA
2021/04/21	Chinese threat actors leverage a new zero-day in Pulse Secure to target US and European organizations
2021/04/21	SonicWall Email Security Targeted with 3 Zero-days
2021/04/22	Trend Micro products are being actively exploited in the wild
2021/04/26	Hacking campaign targets FileZen file-sharing network appliances
2021/04/30	F5 Big-IP Vulnerable to Security-Bypass Bug
2021/04/30	New ransomware group uses SonicWall zero-day to breach networks

The second ‘trend’ we mentioned in last month’s report concerns security vulnerabilities in Apple’s iOS, noting that the **Apple iOS operating system** has been featuring more and more in our advisories over the last 12 months. We did not report any more iOS issues during April, though we did report an Apple Patch for a **Zero-Day MacOS Bug** That Can Bypass Anti-Malware Defenses.

A peek ahead at May to date reveals another two iOS zero-day vulnerabilities and further threats involving Pulse Secure, so we will continue to monitor both of these trends.

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.



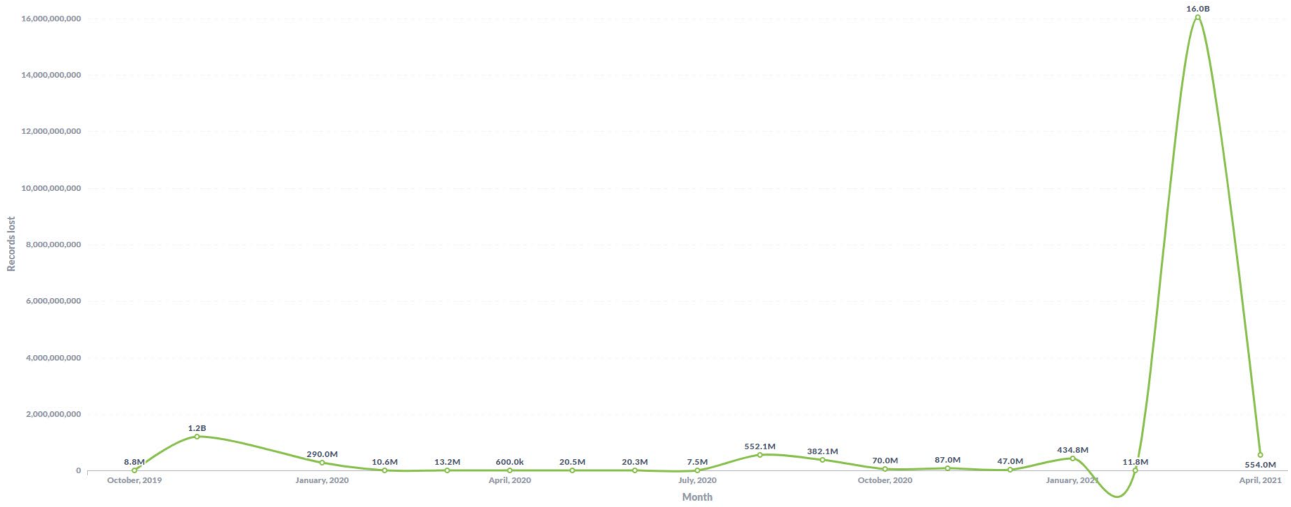
Major breaches recorded over time

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

April was seemingly a quieter month for data breaches as we saw a significant drop in the number we reported on, with only 7 Signals being categorised as a Breach. We appear to be seeing peaks and troughs in terms of the number of breaches seen, however the trendline is still following an upward trajectory and we expect that to continue.

Notable this month was the **attempt by the REvil criminal group to extort money from Apple following the compromise of Original Device Manufacturer (ODM) Quanta Computer**. Apparently, Quanta refused to engage with the group when they demanded a $50 million dollar ransom, so the group threatened to sell or leak blueprints of Apple devices they claimed to have stolen, and suggested Apple should pay them instead. The final outcome of this is not currently known, REvil did reduce their demand to Quanta to $20 million dollars and set a new deadline, this has now passed though and there is no longer a listing on the REvil leak site.

Another interesting breach was seemingly a case of criminals attacking criminals when **the database from cybercrime forum Swarmshop was published on another underground forum.** The admins behind Swarmshop, primarily a place to trade payment card information, attributed the database to a previous breach that occurred in January 2020 however analysis showed records with more recent timestamps. It is not clear who was behind this breach, but it is thought to be a case of a revenge attack or a competitor trying to discredit them.

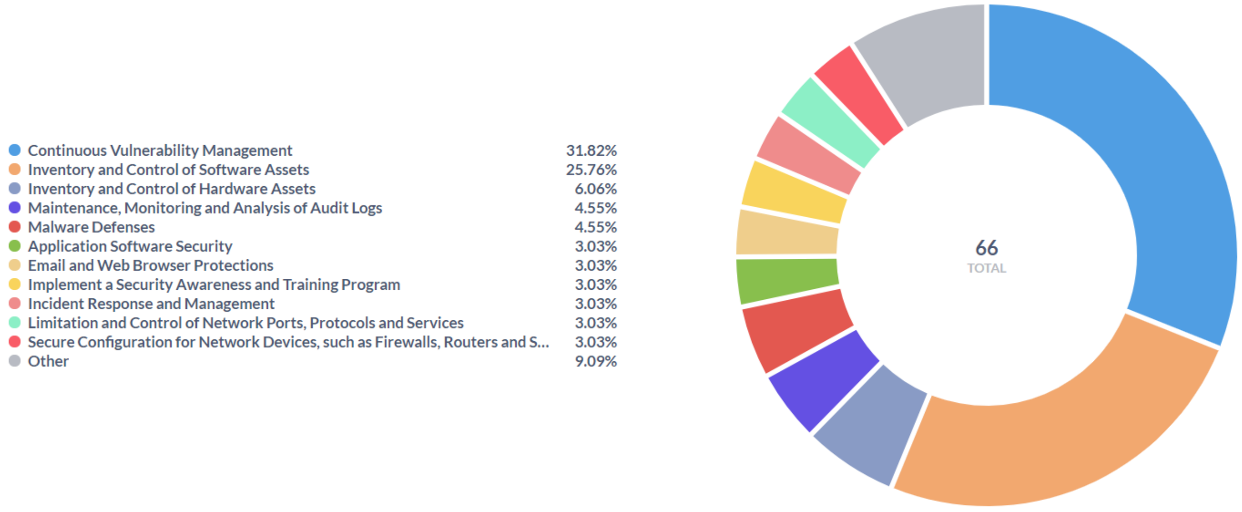


Breached records identified in our analysis over time

You can see in the chart above that **April actually saw the second highest number of stolen records in our dataset**, with 554 million records stolen. This excludes the anomalous figure for March, which significantly skewed our data.

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 during April

This chart summarises the recommendations our analysts have made in our Signals during the month of April. In what is a recurring theme the basic CIS controls concerning Vulnerability Management and Inventory of Software & Hardware maintain their top 3 positions. **'Maintenance, Monitoring and Analysis of Audit Logs'** also features prominently. We believe this is a key component in any environment, you cannot take a 'fire and forget' approach to your security solutions and other systems, they must be monitored and maintained in order to ensure effectiveness thus allowing you to detect attacks in progress providing you respond to any alerts they may generate.

With an equal volume of recommendations though you can see the foundational CIS controls of **'Email and Web Browser Protections'** & **'Limitation and Control of Network Ports, Protocols and Services'** along with the organisational controls of **'Implement a Security Awareness and Training Program'** & **'Incident Response and Management'**.

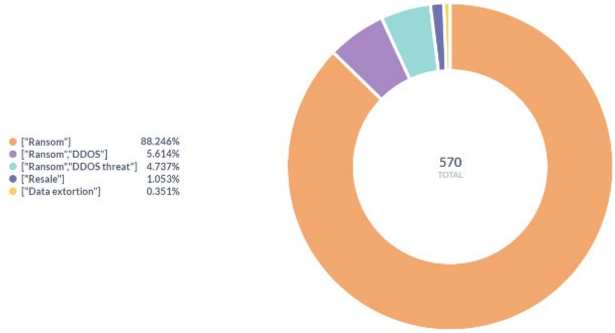
These elements are all recommendations we also make in our recent webinar on beating ransomware, **'Don't be a victim. Ransomware can be beaten!'**, this can be seen on demand here https://orangecyberdefense.com/global/events/beat-ransomware-stop-losing-money-time-and-reputation/. We also go into a lot more detail in the associated comprehensive paper that you can register to download here https://orangecyberdefense.com/global/white-papers/beating-ransomware/.

Cyber Extortion Trends (Beta)

Summary

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

- In April we saw the highest number of leaks so far within one month at **157**.
- Avaddon continued to increase their activity in April, being in spot top 2 of all activity we are monitoring in 2021.
- All April leaks originated from 12 leak sites, while we actively monitor a total of 22 leak sites
- BABUK made several announcements, concluding that **they will move towards data extortion only, and no longer encrypt systems and files.**
- We added several new leak sites during April, (N3tworm, LV blog 2, Lorenz). Unfortunately, **this trend of victim shaming seems to be successful and others are joining in.**
- We witnessed some re-branding (e.g. MountLocker to Astro Team), re-sharing of victim information (e.g. MountLocker, Astro; Marketo)
- We're **seeing marketplace sites popping up, as a last attempt to sell the data of victims** that chose not to pay (e.g. Marketo, Dark Leak Market)



- We added two new attack types due to the mentioning above, we now differentiate between ransomware attack 'Ransom', DDOS and DDOS threatening (used by attackers to increase pressure and the likelihood of payment). We also **added re-sale and data extortion as attack categories.**
- In April we have an increase in the volume of public administration sectors being targeted (Small municipalities in Italy, Portugal, Canada and Spain, Government of Fiji, Police Department DC, etc.)
- We observed a few victims from Czech Republic and even Romania, which we don't come across often.
- The top 3 countries targeted in April: US (46.5%), GB (7.64%) and FR (6.37%).

What's in a name?

To counter the ransomware threat, we need to first understand **what** ransomware is. While the term "ransomware" is generally understood, it falls short of wholly capturing a complex and evolving issue. Let's take a moment to clarify the common terms so that we may propose a definition that better suits our needs:

Malware: any software that has been designed to operate in a malicious, undesirable manner, without the informed consent of the computer owner or user.

Ransom: a consideration paid or demanded for the release of someone or something from captivity[1].

Ransomware: malware that holds the data of a computer user for ransom.

Big game hunting: a targeted ransomware operation that involves infiltrating large corporate or government networks that will be significant and lucrative.

Extortion: is the act or practice of wresting anything from a person by force, duress, menace, authority[2].

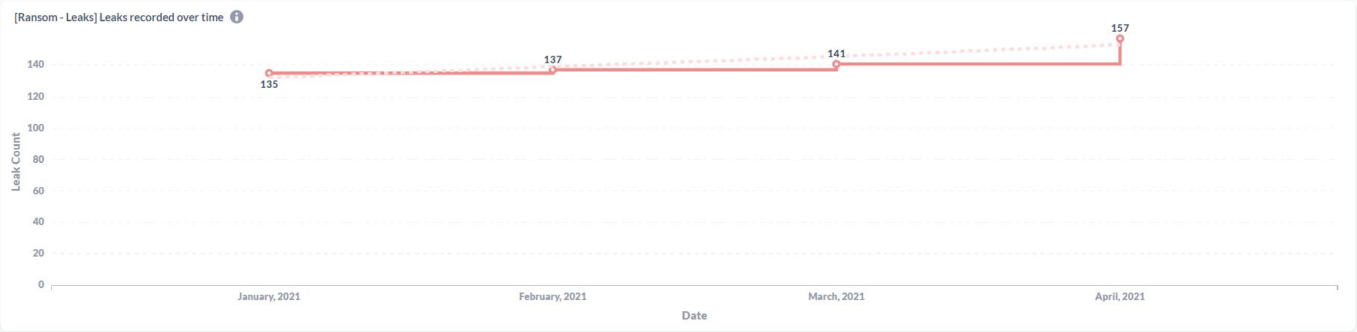
These definitions all accurately describe the evolution of the criminal business model and the challenges we have faced thus far. However, the terms malware, ransomware, double extortion, data and even ransom have not remained consistent during the evolution of this crime.

What does appear to be consistent in this form of crime is the notion of extortion. At the heart of the ransomware crimewave is the basic idea that if you take something unique and precious from someone, they'll pay to have it back. If you discover someone's secret, they'll pay you to keep it secret. If they consume all your bandwidth, you'll pay them to stop. The microcosmic market of one seller and one desperate buyer involved in these acts of extortion drives immense profits for the criminal.

The term double extortion describes a specific form of ransomware attack, but it doesn't make for a good general definition. To capture the history, current form, and potential future of this insidious form of cybercrime, we therefore propose to use the term "**cyber extortion**" or 'extortion' for these reports.

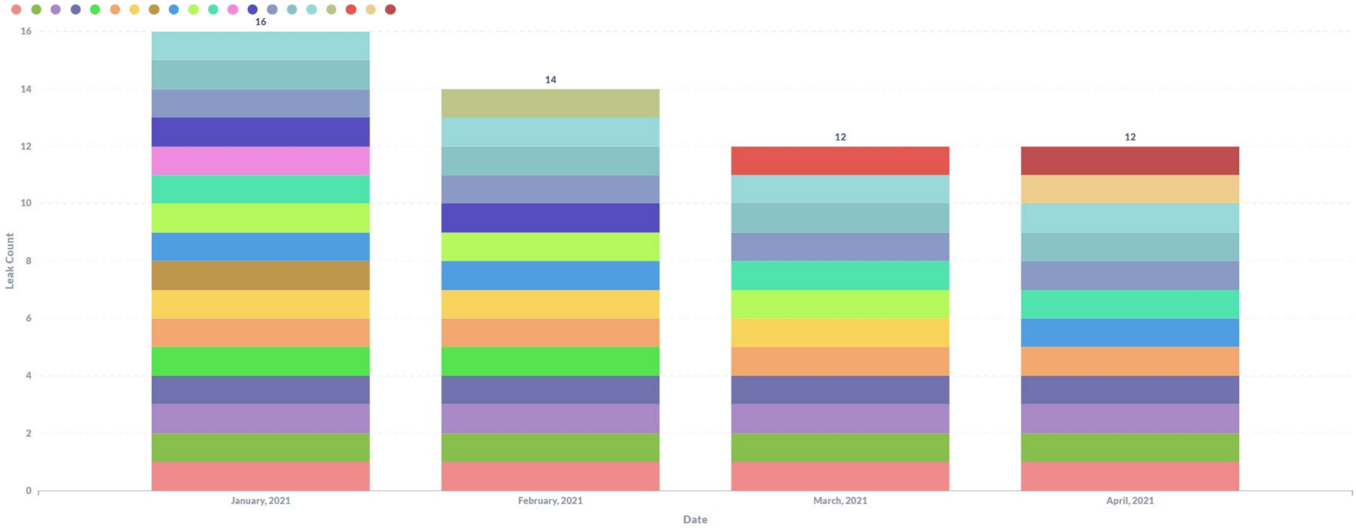
General Trends

Through our ransomware leak site monitoring program we have succeeded in documenting a set of **570 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

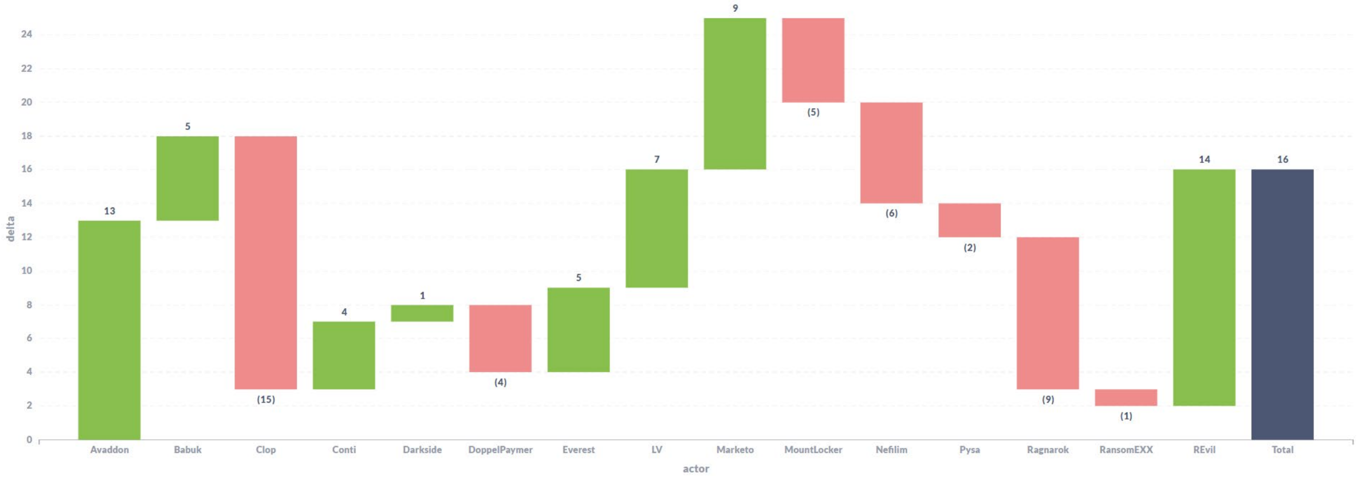
The total number of leaks we have been able to observe has grown by about 11% in April over March. This increase may be due to two new actors we started tracking in April, increasing our list of actors under observation from 18 to 20. As the chart below shows, however, the number of unique active actors who have been active from month to month has actually decreased since we started the project.



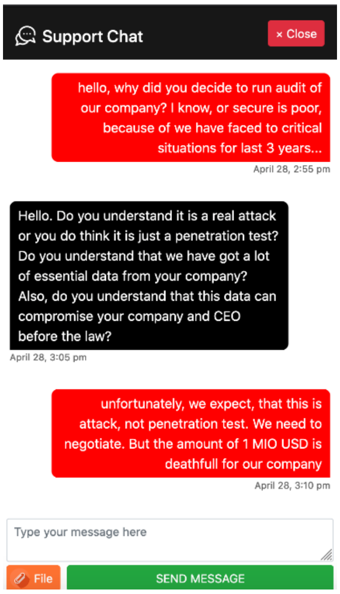
Unique active ransomware actors observed per month

It’s probably too early in this dataset to derive any theories regarding larger trends, however.

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



Ransomware actors - changes since March



hello, why did you decide to run audit of our company? I know, or secure is poor, because of we have faced to critical situations for last 3 years...

April 28, 2:55 pm

Hello. Do you understand it is a real attack or you do think it is just a penetration test? Do you understand that we have got a lot of essential data from your company? Also, do you understand that this data can compromise your company and CEO before the law?

April 28, 3:05 pm

unfortunately, we expect, that this is attack, not penetration test. We need to negotiate. But the amount of 1 MIO USD is deathfull for our company

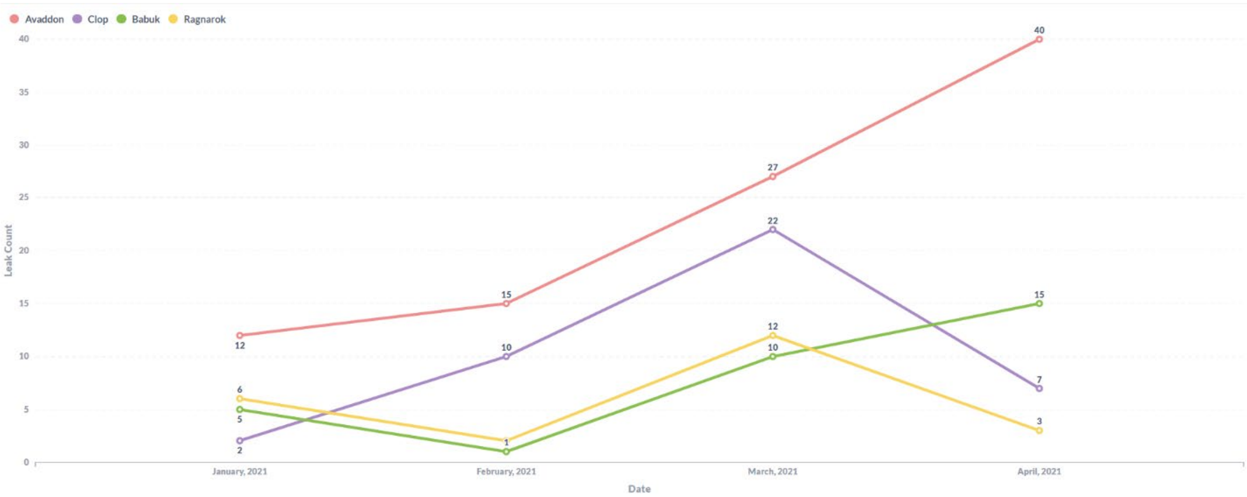
April 28, 3:10 pm

As the chart above illustrates, there have been some big winners and losers among the players this month:

- Avaddon has increased their substantial March tally from 27 to 40 victims in April.
- REvil increased their tally by 14 to 31 victims in April.
- Marketo hit the scoreboard in April with an increase of 9 victims.
- Cl0p on the other hand dropped 15 from 22 victims in March to only 7 in April.
- Ragnarok also slipped by 9 from 12 victims in March to only 3 in April.

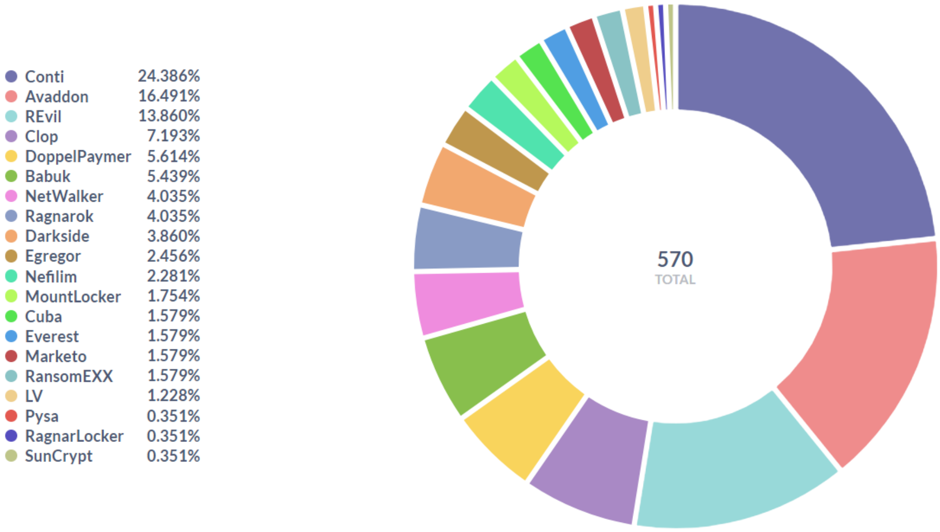
In last month's report we noted a decrease in compromises by the major players – Conti, DoppelPaymer, and REvil, but a significant increase in activity by Avaddon and Babuk.

We revisit the performance of these players again below.



Avaddon & Babuk still growing, Cl0p & Ragnarok set back

The net effect of these new leaks reveals the relative position of the 20 players we're monitoring as follows:



Ransomware leaks by Actor – YTD 2021

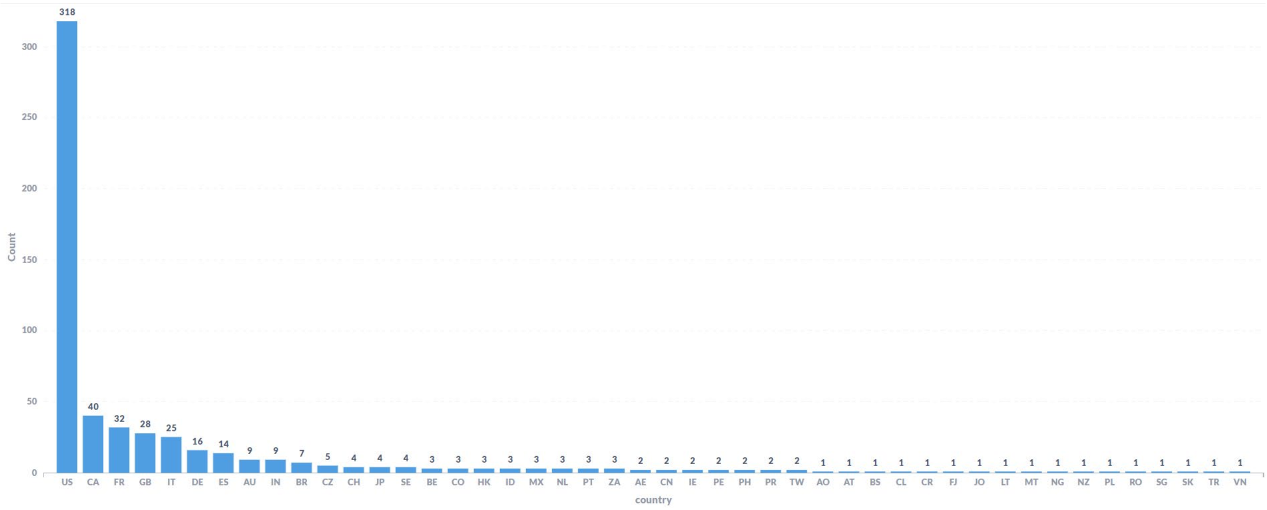
We note that the high level of activity by Avaddon has moved them from 4th to 2nd place over the last two months, while REvil has dropped from 2nd to 3rd.

Victimology

The familiar patterns in victimology persist.

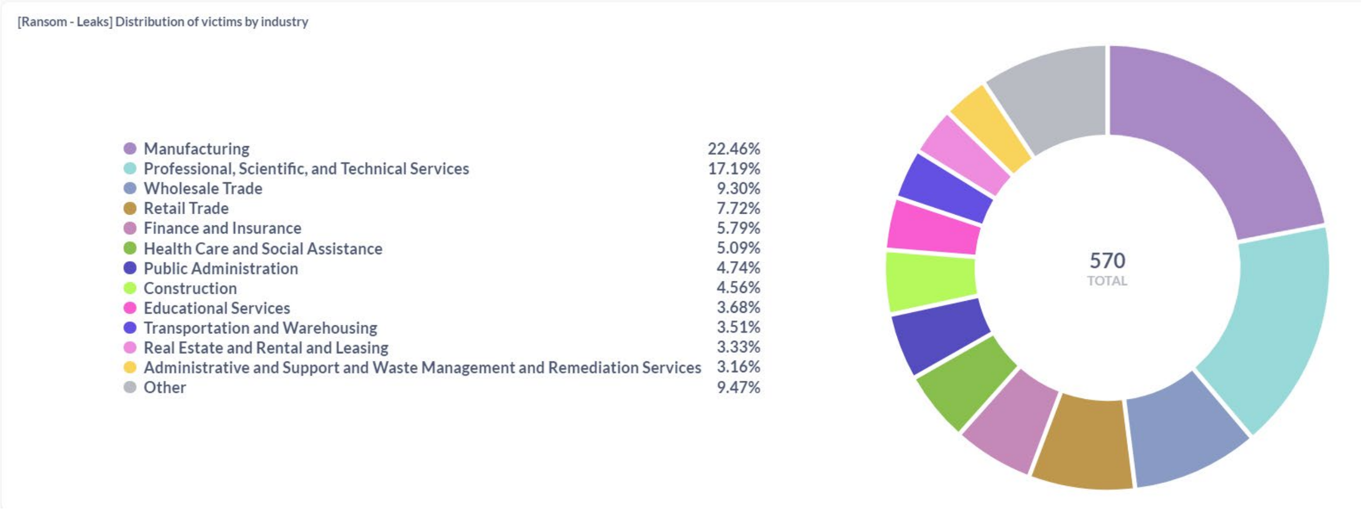
In our March report we noted volumes of incidents impacting Italian and French businesses. In France we had observed a massive spike in compromises during March, but in April the number of French victims dropped again from 14 to 10. In Italy, however, the number of monthly victims increased by 1 from 7 to 8.

The distribution of leaks across our entire dataset therefore now looks as follows:



Recorded leaks by Country– YTD 2021

We note that the victim country patterns broadly track the size of the country's economy. Some countries appear to be notably underrepresented, but **for developed countries generally it seems safe to say that the victims of double extortion can be found everywhere.**

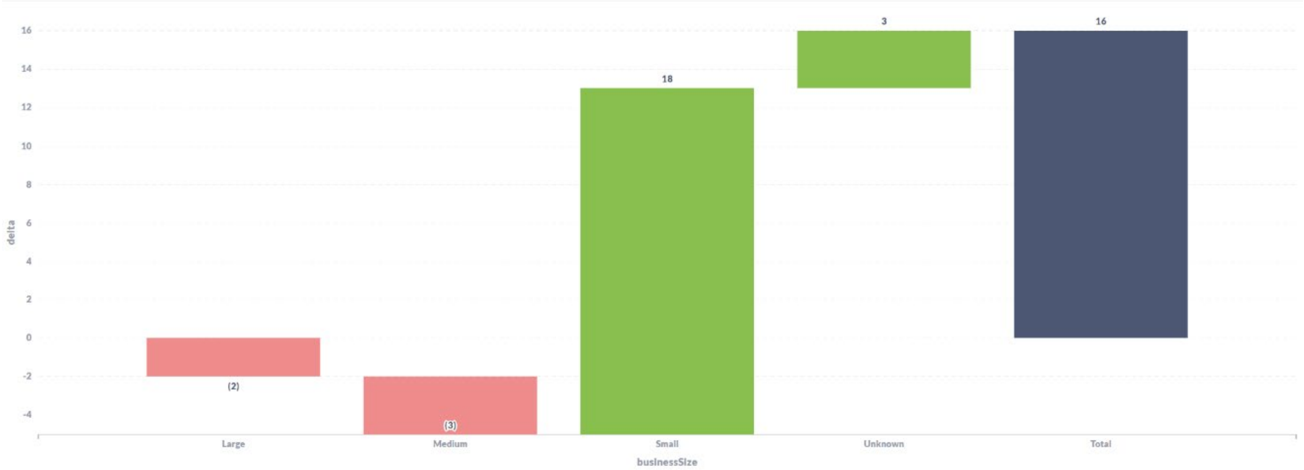


Recorded leaks by Industry– YTD 2021

The distribution across Industry segments appears to be a clearly emerging pattern – Manufacturing and Professional Services firms consistently appear to be the most frequently hit, although the distribution does shift somewhat from month to month. The notable 'swings' in terms of Industry during April were:

- Manufacturing – increased 30 in March to 43 in April
- Public Administration – increased from 3 in March to 12 in April
- Wholesale – increased from 8 in March to 12 in April
- Professional Services decreased from 28 to 20.

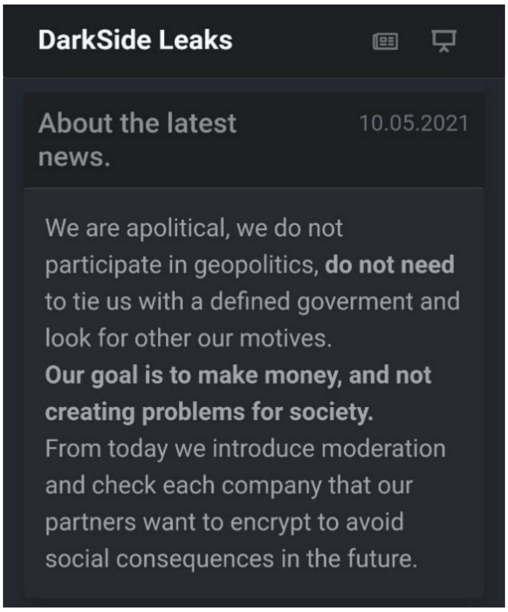
The pattern in terms of business size appears to be cementing even further:



Changes in recorded leaks by victim size – April 2021

Our dataset suggests that more than 70% of the leak site victims are 'Small' businesses, and during April the number of victims in this category grew even further.

Colonial Pipeline and DarkSide



DarkSide Leaks

About the latest news. 10.05.2021

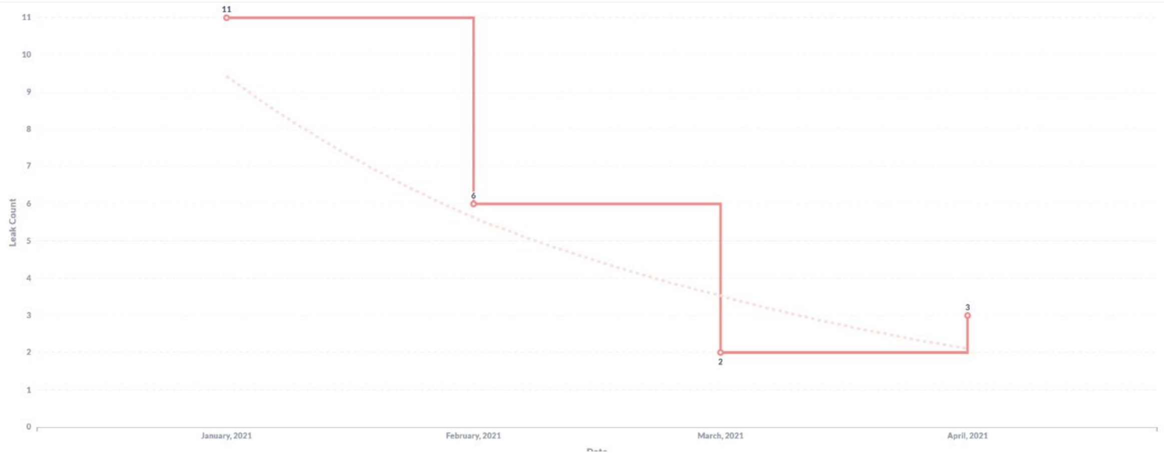
We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

On May 11th, just as this report was ready to release, we reported that Colonial Pipeline, the largest fuel pipeline in the United States, had shut down operations after suffering what was reported to be a ransomware attack attributed to the DarkSide extortion group, which we monitor.

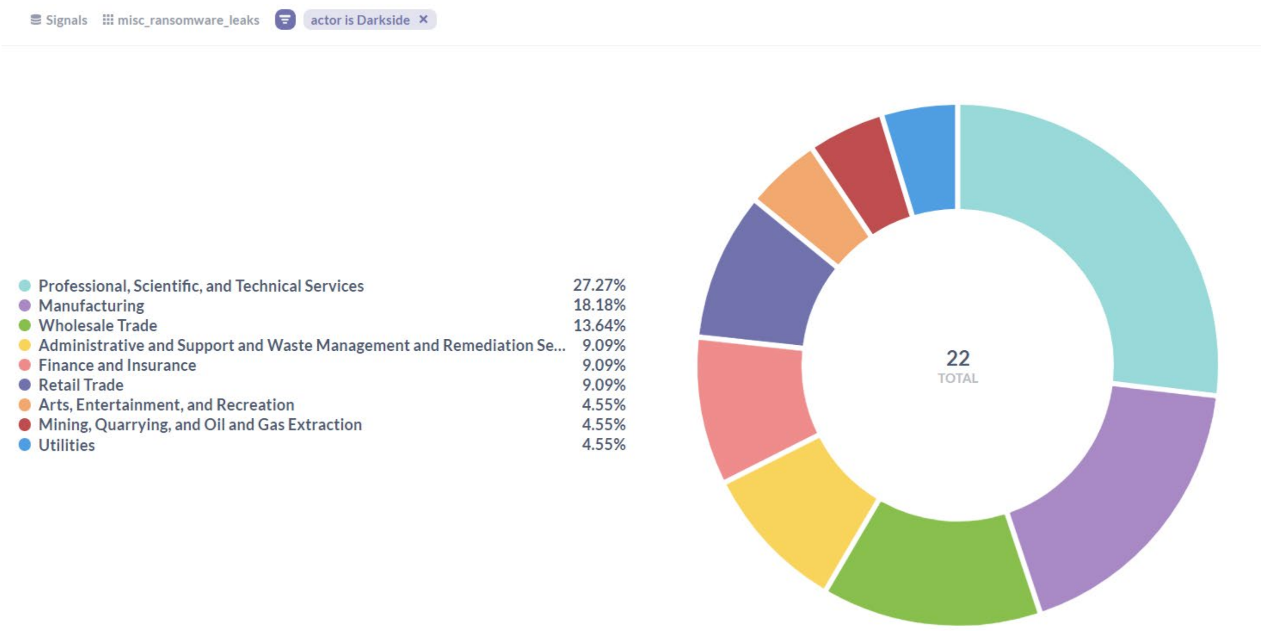
The Colonial Pipeline incident appears thus far to be standard double-extortion, and the group themselves have announced (see screenshot on the left) that they operate purely for financial grounds and have no political affiliation. This is a more complex issue than DarkSide might like to think, which is a subject we may be able to explore further in next month's report.

There's no doubt that we will have a better understanding of the attack and its implications in time for next month's report also. Since the actor is known to us, however, we are able to provide some insight into their operations here.

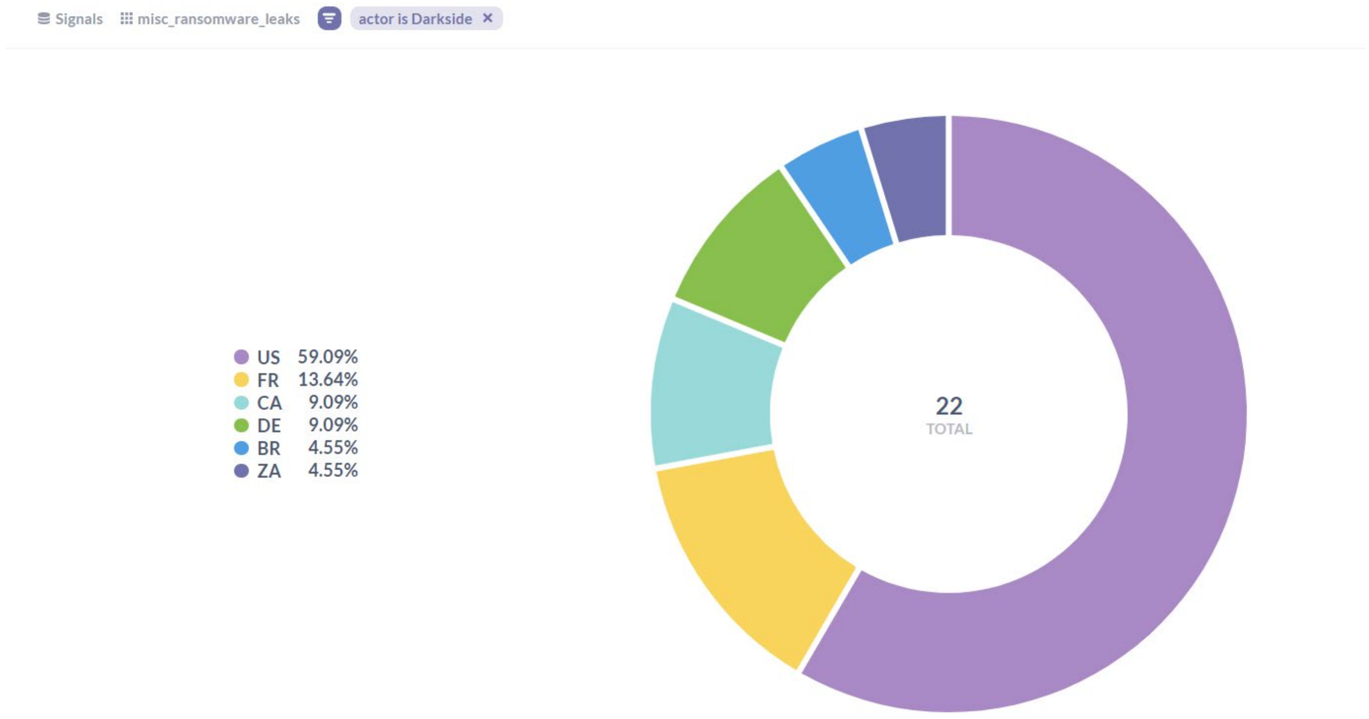
DarkSide has been active since at least August 2020, but of course we have only been actively observing them since January this year.



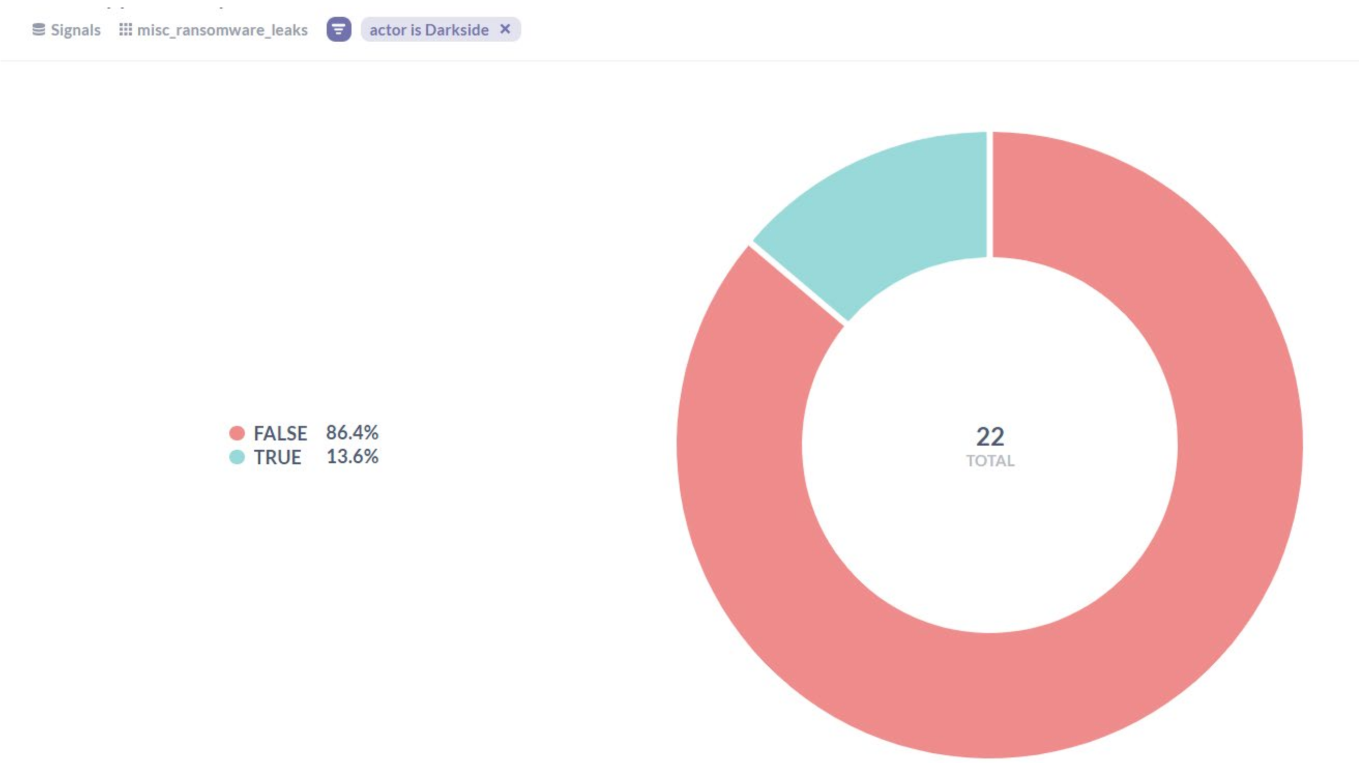
DarkSide activity appears to have been decreasing over time



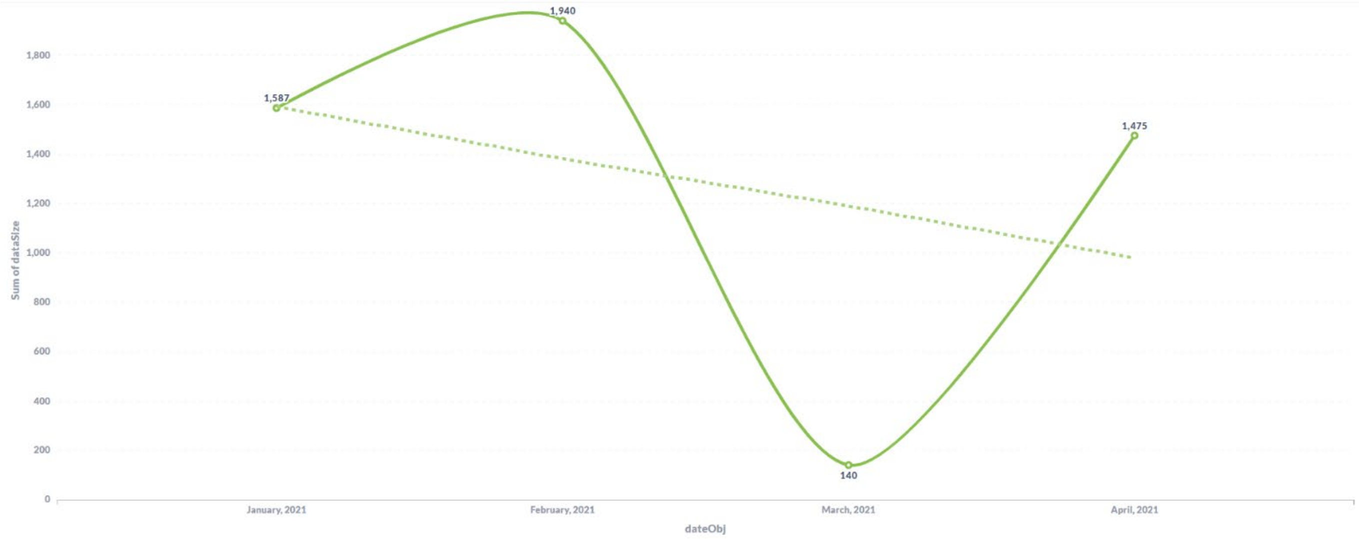
DarkSide's 22 victims mirror the general Industry patterns



DarkSide's 22 victims mirror the general Country patterns



DarkSide’s payment success rate is about 14%, a little above average



DarkSide’s volumes of data extorted varies from month to month

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:

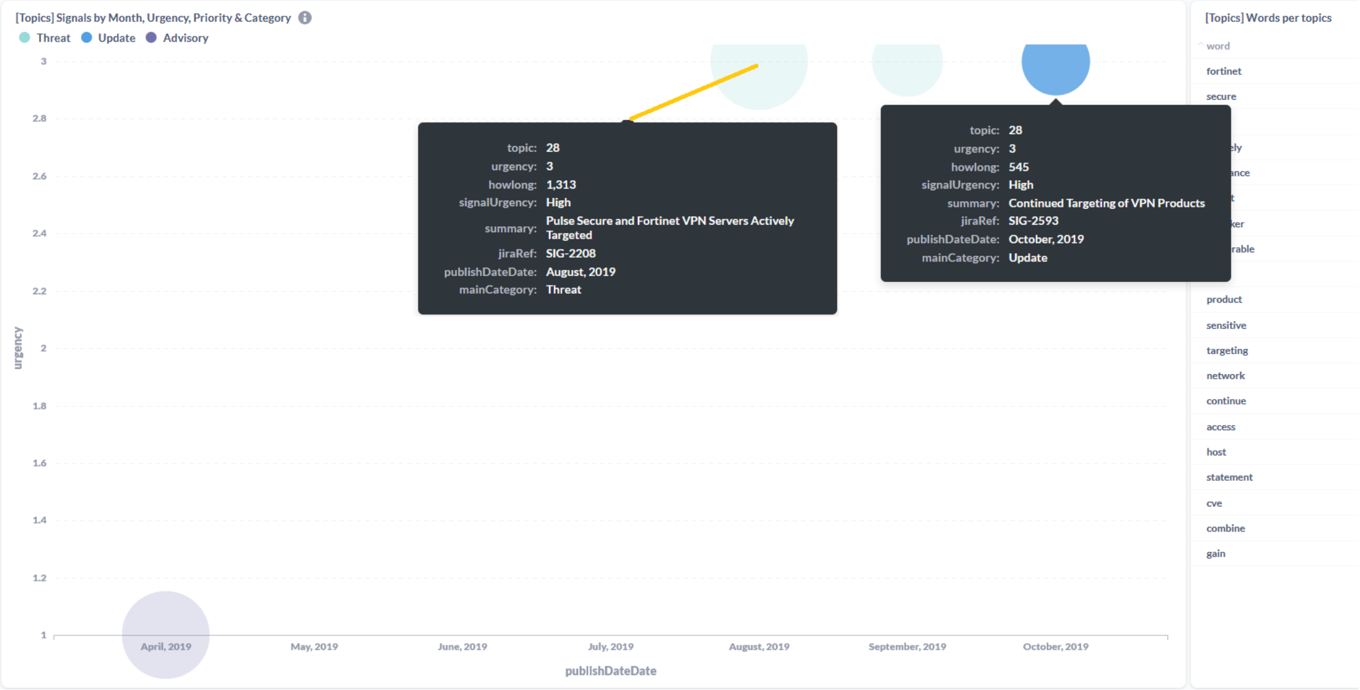
The topic modelling algorithm looks for sets of matching words and phrases across all our Signals and then groups the Signals together according to ‘topics’. The algorithm doesn’t know what the ‘topics’ refer to, only that the Signals grouped by those topics use similar language.

This month contained several stories involving Secure Remote Access technologies. Our topic model has created a grouping with a strong focus on a particular VPN vendor.

In April 2019 we published SIG-444 that listed several fixes for VPN products. Included in this was an announcement for security fixes for Pulse Secure products. Later that same month Pulse Secure published security fixes for Pulse Connect Secure that included a fix for a vulnerability tracked as CVE-2019-11510. At the time this was just another vulnerability that need to be patched.

A couple of months later this changed, with Orange Tsai and Meh Chang presenting their talk ‘Infiltrating Corporate Intranet Like NSA - Pre-auth RCE on Leading SSL VPNs’ at Black Hat USA 2019. Since this talk Secure Remote Access technologies have been increasingly in the attacker’s sights. We published SIG-2208 to cover this announcement.

This can be illustrated by looking at how the topic model grouped specific Signals sharing similar messaging. To see how this grouping evolved we start by examining a grouping for November 2019:



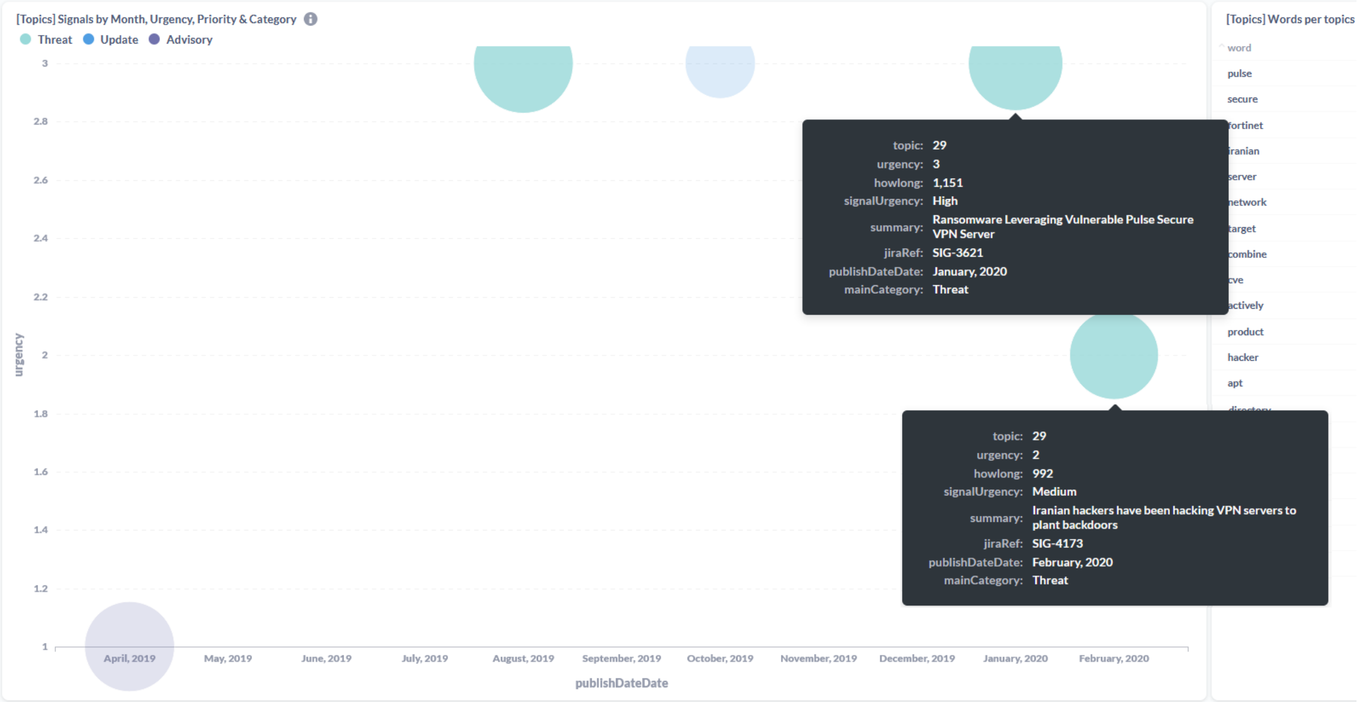
topic: 28
urgency: 3
howlong: 1,313
signalUrgency: High
summary: Pulse Secure and Fortinet VPN Servers Actively Targeted
jiraRef: SIG-2208
publishDateDate: August, 2019
mainCategory: Threat

topic: 28
urgency: 3
howlong: 545
signalUrgency: High
summary: Continued Targeting of VPN Products
jiraRef: SIG-2593
publishDateDate: October, 2019
mainCategory: Update

[Topics] Words per topics

word
fortinet
secure
ely
ance
t
ker
rable
product
sensitive
targeting
network
continue
access
host
statement
cve
combine
gain

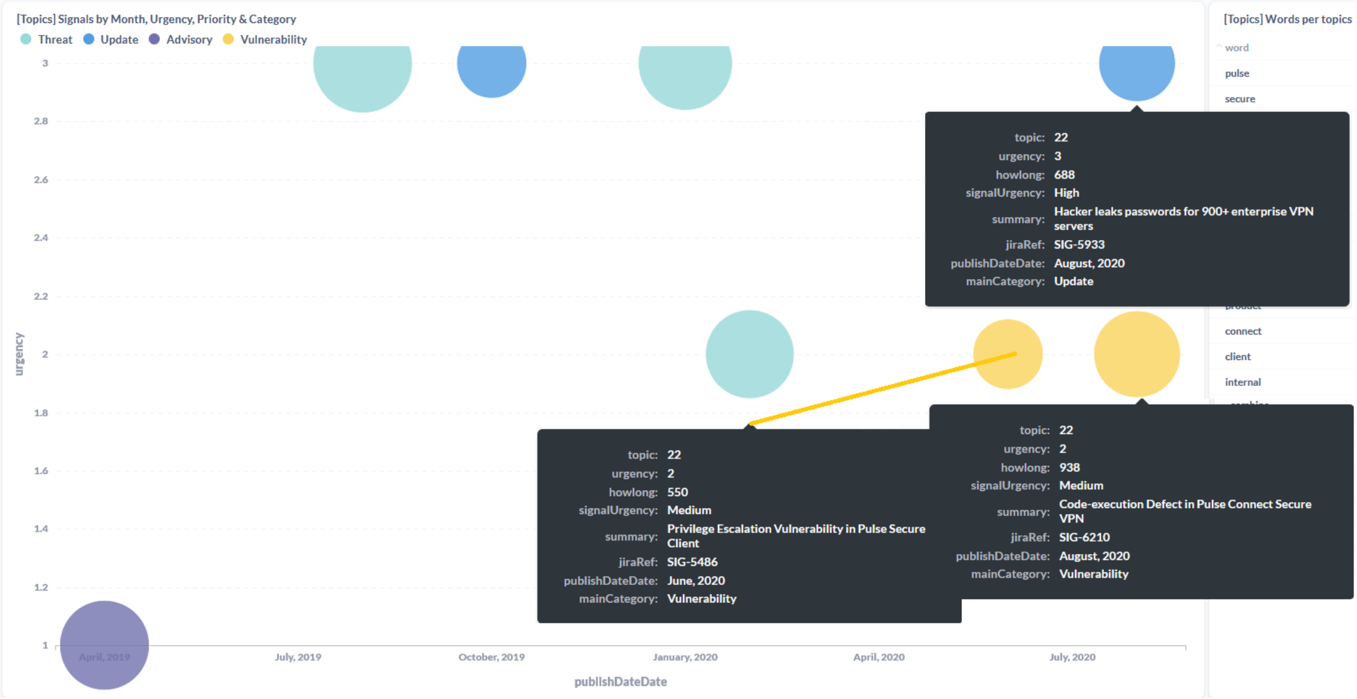
Fast forward to February 2020 and we see that attackers have started to leverage these VPN vulnerabilities:



topic: 29
urgency: 3
howlong: 1,151
signalUrgency: High
summary: Ransomware Leveraging Vulnerable Pulse Secure VPN Server
jiraRef: SIG-3621
publishDateDate: January, 2020
mainCategory: Threat

topic: 29
urgency: 2
howlong: 992
signalUrgency: Medium
summary: Iranian hackers have been hacking VPN servers to plant backdoors
jiraRef: SIG-4173
publishDateDate: February, 2020
mainCategory: Threat

If we jump to August 2020, a year after the Black Hat USA 2019 talk, we see more activity involving VPNs. Here the topic model included vulnerabilities along with attacks:

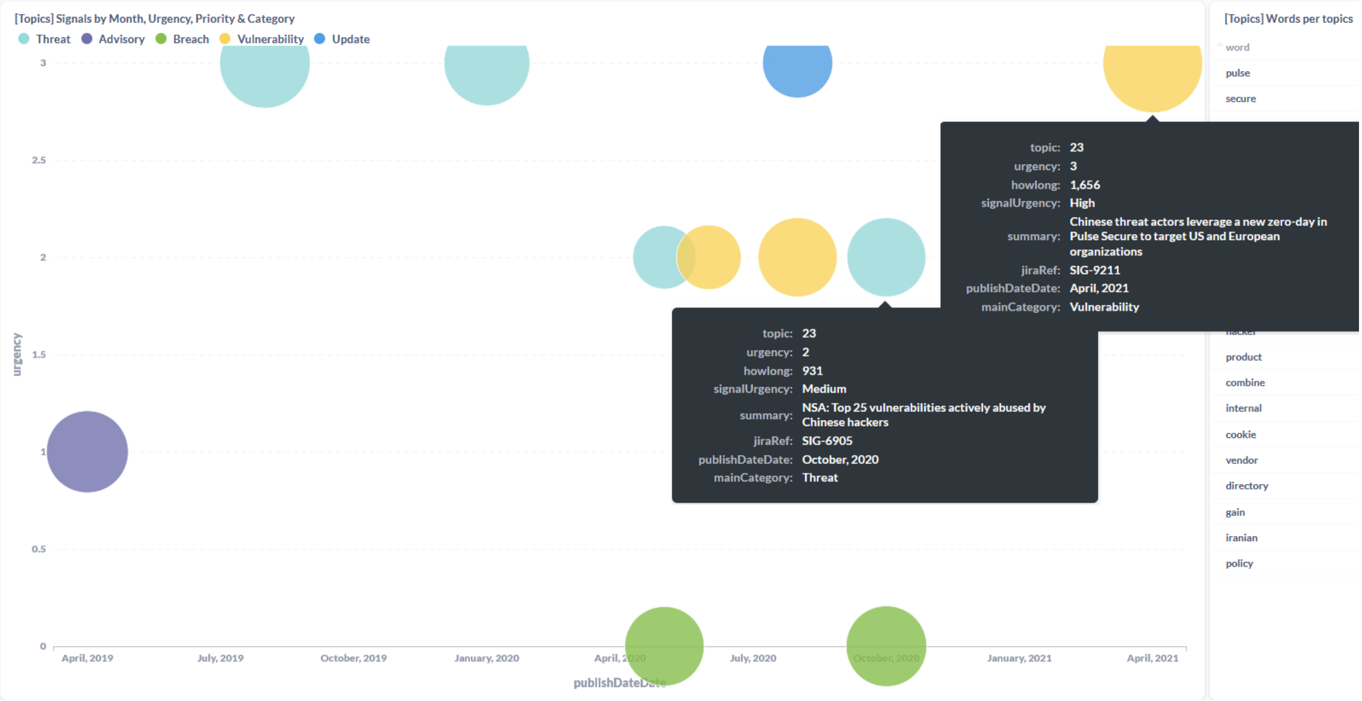


topic: 22
urgency: 3
howlong: 688
signalUrgency: High
summary: Hacker leaks passwords for 900+ enterprise VPN servers
jiraRef: SIG-5933
publishDateDate: August, 2020
mainCategory: Update

topic: 22
urgency: 2
howlong: 550
signalUrgency: Medium
summary: Privilege Escalation Vulnerability in Pulse Secure Client
jiraRef: SIG-5486
publishDateDate: June, 2020
mainCategory: Vulnerability

topic: 22
urgency: 2
howlong: 938
signalUrgency: Medium
summary: Code-execution Defect in Pulse Connect Secure VPN
jiraRef: SIG-6210
publishDateDate: August, 2020
mainCategory: Vulnerability

A strong theme has developed for this grouping. With this analysis we see that the **intelligence published in October 2020 by the NSA was accurate when we look at the Signal we published in April 2021. SIG-9211 covered a zero-day in in Pulse Connect Secure being exploited by an attacker with strong links to the Chinese government.**



topic: 23
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: 23
urgency: 2
howlong: 931
signalUrgency: Medium
summary: NSA: Top 25 vulnerabilities actively abused by Chinese hackers
jiraRef: SIG-6905
publishDateDate: October, 2020
mainCategory: Threat

word
pulse
secure
hacker
product
combine
internal
cookie
vendor
directory
gain
iranian
policy

The two green circles represent breaches covered by SIG-5152 and SIG-6829. In both Signals we reported that Bad Packets found out of date Pulse Connect Secure servers that were part of the infrastructure of both victims. There was no indication that these Pulse Connect Secure servers were leveraged in either breach, however.

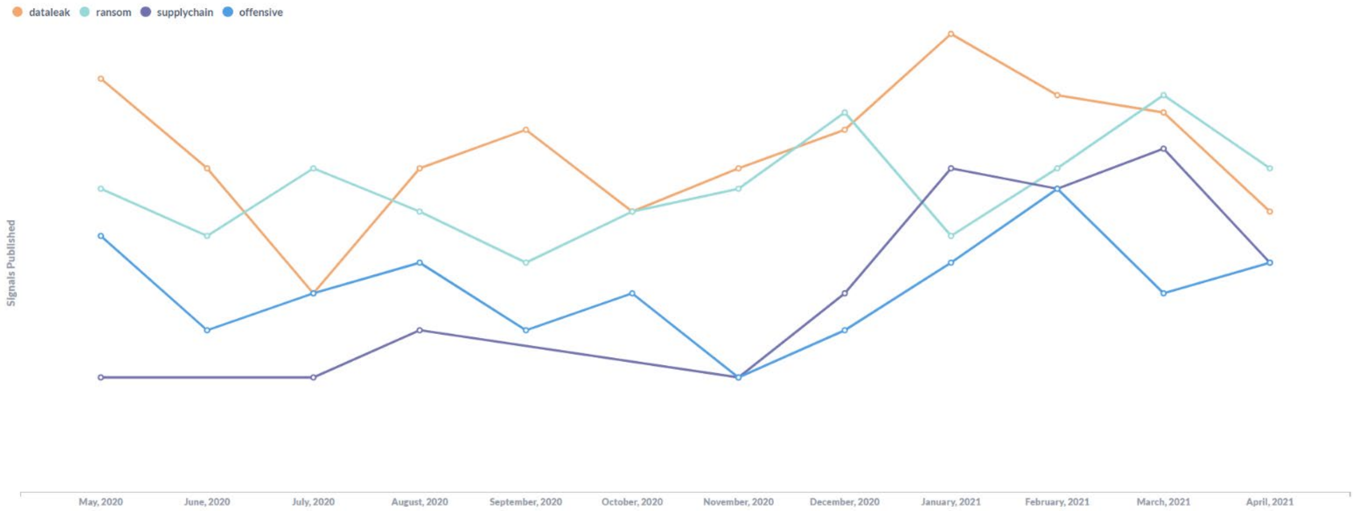
If this trend continues then the latest set of zero-days in Pulse Connect Secure products, covered in SIG-9211, will be used by other attackers. We anticipate that ransomware groups may be lining up to take advantage of this.

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.

Dataleaks, cyber extortion, supply chain attacks and government hacking

This month we revisit some general trends that have been occupying our collective attentions for some time now – dataleaks, cyber extortion, supply chain attacks and government hacking operations….



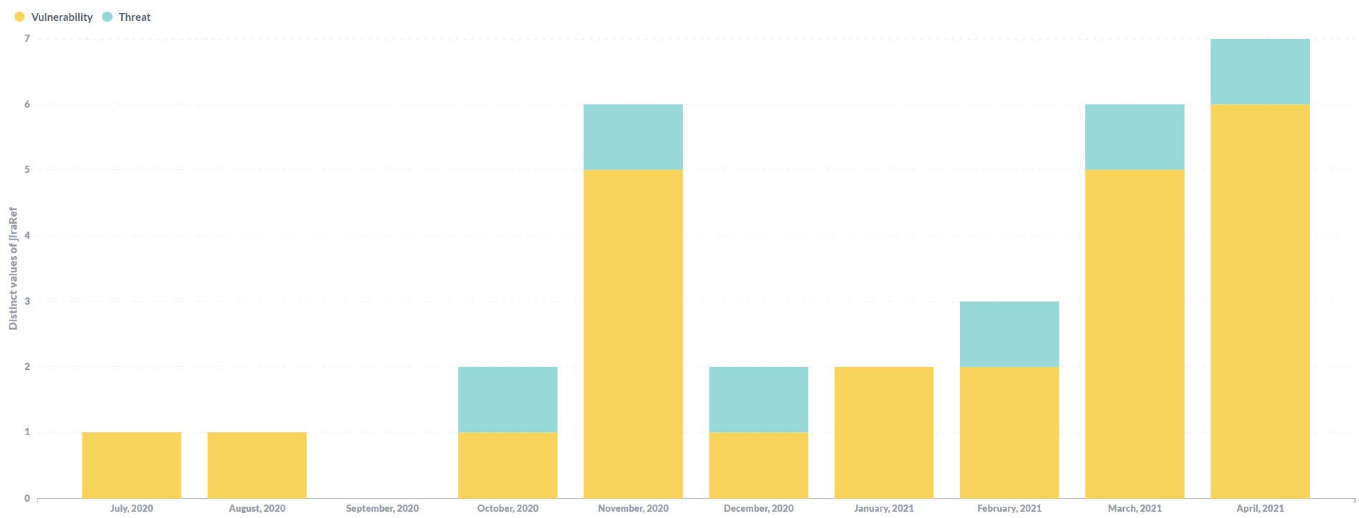
Several major trends slowed during April

The graph above tracks the number of Advisories we have published that were tagged with trend markers representing the key systemic factors we track in the security landscape. Basically, it illustrates how often major themes occur in the Advisories we publish each month. Month by month variations are arguably too small to draw serious inferences from, but the following observations can probably be safely made:

- Advisories concerning **dataleaks and cyber extortion (ransomware) appear to be trending slightly downwards since January.** Certainly, the inexorable upward trajectory we experienced during H2 of 2020 appears to have slowed since the start of this year.
- Advisories concerning **Supply Chain security issues spiked strongly after the SolarWinds incident in December last year.** We saw a dip in this trend in February and then another significant drop in April, although we still covered this topic in our Advisories in April more than at any point last year.
- **Advisories making reference to government hacking operations slowed through the COVID-19 pandemic but started climbing again at the end of last year.** After a big dip in this theme in March we noted a slight increase in activity again in April. The monthly volume of advisories involving this theme is now at about the same level as before the pandemic, and it will be interesting to note how it develops from here.

Zero-days becoming a growing threat?

A newly emerging trend that is worth monitoring is the growing prevalence of 'zero-day' vulnerabilities and threats in our advisories, as the graph below reveals.



Zero-day threats and vulnerabilities become more prevalent

We have noted that zero-day exploits appear to be playing a bigger role in attacks and compromises than before, and the chart above, which roughly tracks the occurrence of the term in our Advisories over time, appears to support that hypothesis.

Zero days are not a new concept but perhaps need to be given more attention in our threat models. **Our security strategies need to assume compromise, deploy defense-in-depth, and be fundamentally intelligence led to ensure that we are well positioned to deal with an attack against which there is no patch.**

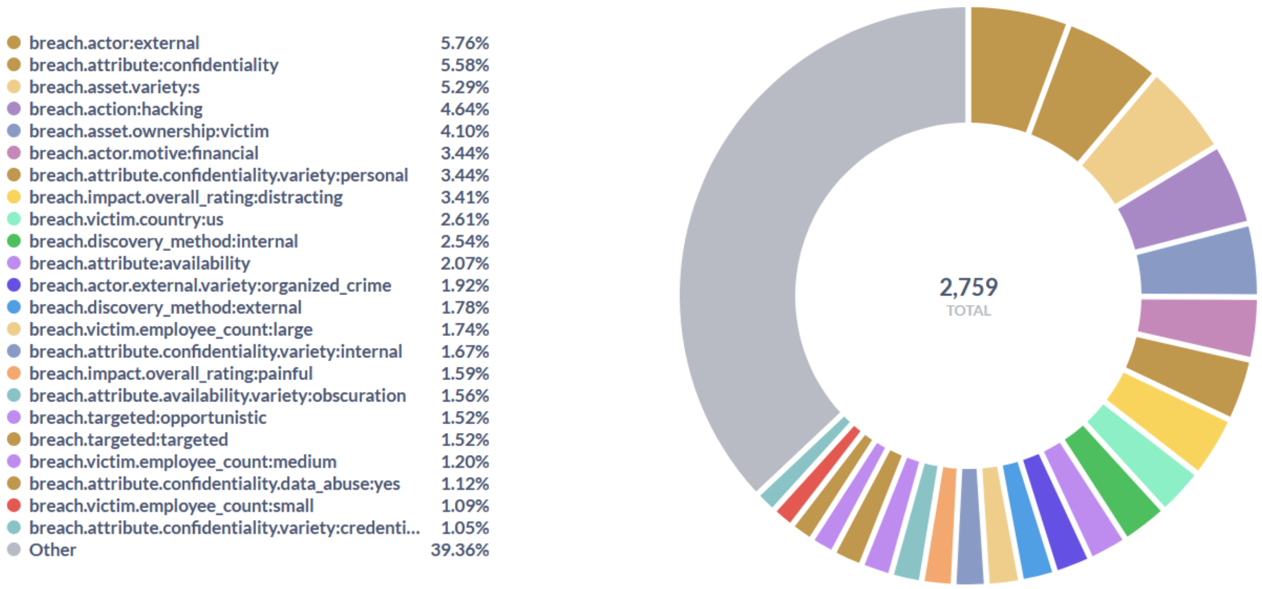
A deep dive into April's tags

We have collected several breach incidents over the past 18 plus months and we have tagged these incidents using a scheme that resembles the Veris tagging taxonomy. These tags give us an ability to annotate an incident as best we can, based on the information that is publicly available.

Using Signals that the topic model picked we can see a pattern emerging regarding data breaches.

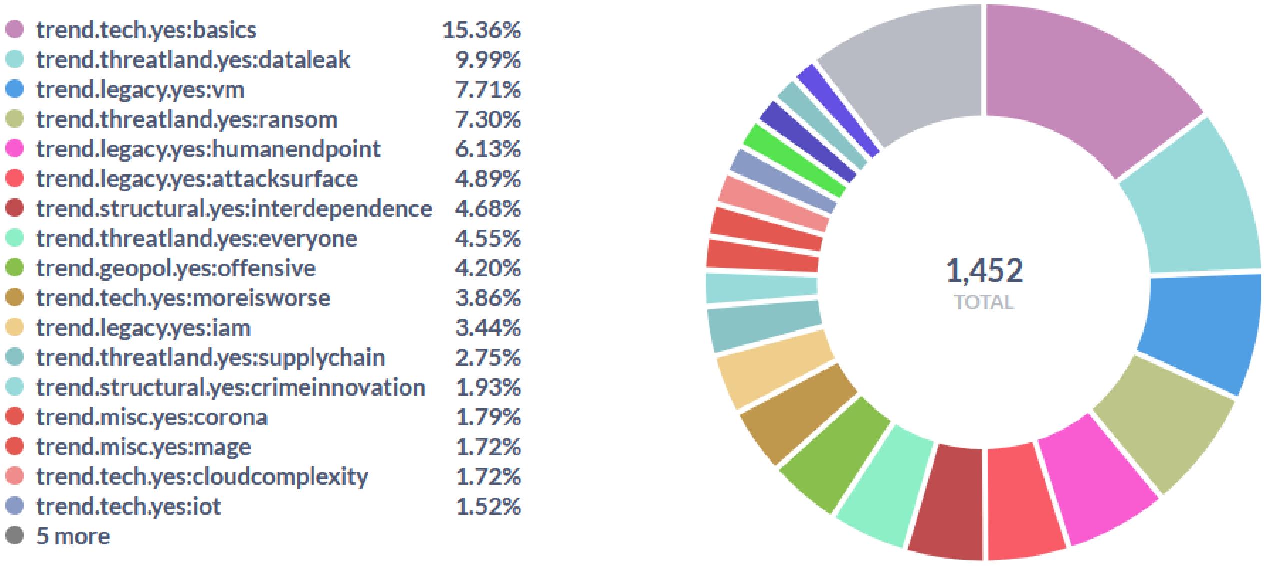
- The pie chart below lists many **incidents involving attacks originating from outside the organisation** (breach.actor:external).
- **Most incidents were financially motivated** (breach.actor.motive:financial).
- The 'obscuration' tag (breach.attribute.availability.variety:obscuration) **indicates the use of extortion or ransomware tactics**, and is generally followed by some form of data leak (breach.attribute.confidentiality.data_abuse:yes and trend tag discussed later).
- These **tactics are the hallmark of extortion groups** of late (breach.actor.external.variety:organized_crime).
- **Attackers do not discriminate** and will target business of any size (breach.victim.employee_count), but they do seem to favour enterprise-size businesses more than others. This preference is likely influenced by the ability to pay large amounts of ransom with the aid of cyber insurance.

- The data shows that **businesses in the United States are being compromised most frequently** (breach.victim.country:us), but our data is biased by the nature of the sources we rely on.
- **Leaked information includes personal identifiable information, internal proprietary information, and credentials** (breach.attribute.confidentiality.variety).



Included in the tagging taxonomy is our own trend tags that we assign to relevant Signals. These trend tags represent our ‘state of the threat’ and are dynamic forces that we anticipate will influence or will emerge over time. We then tag Signals with the trend tags to track those predictions.

Using the same approach that we followed with the breach tags, we can examine the trend tags and learn what forces are at play. These trend tags are associated with the Signals for April 2021. This is the same Signal sample that was used above to discuss the breach tags.



- Over **15% of our Signals include the 'basics' tag** (trend.tech.yes:basics). This tag speaks to risks, threats, or well-known issues such as phishing, human error, weak passwords, basic vulnerability management challenges, network segmentation, web application security, traditional malware, and more. The 'basic' tag will sometimes also appear with other trend tags that annotate the Signal with more specific tech or legacy tags.

- The **'data leak' and 'ransom'** tags speak to actual risks or threats that are dominating the current threat landscape. Combined, these two tags dominate the 'threat landscape' category and represent over 17% of the total number of tags listed.

- The 'vm' (vulnerability management), 'humanendpoint', and 'iam' (identity access management) tags are generally used with the 'basics' tag mentioned earlier. The 'vm' and 'iam' tags are used to indicate that patches are available but were not deployed or that IAM solutions such as 2FA would have mitigated the incident, if used. The presences of these tags shows that **phishing and the exploitation of vulnerabilities with known security patches remain common attack vectors**.

- The 'moreisworse' tech tag is used to indicate issues with security products, such as Secure Remote Access technologies. Here the 'moreisworse' tag ties nicely in with Signals we published involving **vulnerabilities in VPN products, such as Pulse Connect Secure**.

- The 'offensive' tag is used on a Signal to denote offensive cyber-attacks, by or against a government. For example, attacks attributed by the United States that publicly states certain incidents were a result of actions by groups with links to the governments of Russia, China, North Korea, Iran, and others will be tagged by this. The data shows that this tag is present in 61 of the 1452 trend tags for the given Signal sample selected. It is unlikely that this trend will diminish as **more governments will seek to use cyberspace to further their agendas**.

We believe that organisations are starting to pay attention given the heightened state of alert surrounding ransomware. We might see organisations respond more quickly than before and patch services exposed to the Internet, including Secure Remote Access services.

Applying security patches is not enough. Attackers do not need to exploit vulnerabilities to breach the perimeter. Attackers can leverage VPNs by simply logging in and gain access to internal network. Our **data shows that credential brute forcing or credential phishing are effective in the absence of Identity Access Management solutions that enforce multi-factor authentication**.

DATA BREACHES

SolarWinds have been in the news for the last four to five months. CISA shared details of a breach they assisted with. The attackers leveraged a weak credentials to VPN into the victim and then proceeded to exploit a vulnerability in SolarWinds Orion. The exploit and incident is unrelated to the supply chain compromise reported in December 2020.

Codecov disclosed a compromise of their platform that resulted in a supply-chain compromise potentially affecting several thousand clients.

Attackers leaking large data sets for free is nothing unusual. We saw a large trove of stolen payment card data leaked when criminals breached a known underground card shop and leaked the data for free. Similarly, attackers leaked data from an Indian online store called BigBasket. Continuing with leaking data for free, Facebook suffered a large data leak that included phone numbers of their users.

533 million Facebook users' phone numbers leaked on hacker forum

Date: 06 April 2021

The mobile phone numbers and other personal information for approximately 533 million Facebook users worldwide has been leaked on a popular hacker forum for free.

623,000 Payment Cards Stolen from Cybercrime Forum

Date: 13 April 2021

Researchers at Group-IB have discovered that the user database of the card shop Swarmshop has been stolen and published on another underground forum.

Code analysis platform codecov hacked to conduct a supply-chain attack affecting thousands

Date: 19 April 2021

Popular developer tool "Codecov.io" announced that a malicious actor successfully hacked their internal systems last January. Codecov provides tools that help developers measure how much of their source code is covered by automated testing, a process known as code coverage, which indicates the potential for undetected bugs being present in the code.

REvil gang tries to extort Apple, threatens to sell stolen blueprints

Date: 22 April 2021

The REvil ransomware gang compromised Quanta Computer and allegedly stole proprietary information linked to several clients one being Apple. REvil asked Apple to "buy back" stolen product blueprints to avoid having them leaked on REvil's leak site before the Apple Spring Loaded event where the new iMac was introduced.

CISA Identifies SUPERNOVA Malware During Incident Response

Date: 23 April 2021

The Cybersecurity and Infrastructure Security Agency (CISA) recently responded to a long-term compromise of an entity's enterprise network. The threat actor connected to the entity's network by logging in to a virtual private network (VPN) appliance and compromised a SolarWinds Orion server by installing malware called Supernova.

Hacker leaks 20 million alleged BigBasket user records for free

Date: 26 April 2021

A threat actor has leaked approximately 20 million BigBasket, an Indian online grocery delivery service, user records containing personal information and hashed passwords.

DigitalOcean data breach exposes customer billing information

Date: 29 April 2021

Cloud hosting provider DigitalOcean has disclosed a data breach after a flaw exposed customers' billing information.

MALWARE AND EXPLOITS

April was a busy month for news involving new threats or malware.

Distributed Denial of Service attacks have evolved according to Akamai. Attackers can now use a new way to generate large volumes data to overload networks of their victims. The attack leveraged an obscure protocol ironically named Datagram Congestion Control Protocol.

ClickStudios disclosed a breach that affected its Passwordstate product. Attackers compromised their software update process and leveraged this to deliver malicious updates to Passwordstate users in the supply-chain compromise.

We published three Signals that relate to attackers exploiting weaknesses in security technologies. Two of these covered ransomware groups using weaknesses in Secure Remote Access technologies to breach victims. Another provided details of an ongoing exploitation of an anti-malware and anti-spam product originally disclosed in middle 2020.

One ransomware group called Babuk decided that extorting the Washington DC Police Department was a good idea. They threatened to release details on gang related police informants if their demands were not met.

We covered two stories involving attackers targeting Linux platforms. One ransomware group announced that they plan on expanding their operation to include Linux hosts. Contrary, a new malware strain was identified that has been lurking on Linux systems for the past 3 years.

Attacks attributed to North Korean affiliated attackers featured thrice. These stories discussed new tools and tactics used by these attackers including the use of images to hide malware payloads.

DCCP, a new DDOS attack vector leveraged by malicious actors

Date: 02 April 2021

According to report released by Akamai, DDoS attackers keep inventing new methods (here using the DCCP protocol) to launch volumetric attacks.

Automated attack abuses GitHub Actions to mine cryptocurrency

Date: 06 April 2021

Attackers have been targeting GitHub repositories, since at least November 2020, that leverage GitHub Actions in order to mine cryptocurrency.

FBI, CISA warn Fortinet FortiOS vulnerabilities are being actively exploited

Date: 06 April 2021

APT groups are suspected of harnessing three bugs, two critical, for data exfiltration purposes.

Ongoing attacks are targeting unsecured mission-critical SAP apps

Date: 07 April 2021

Threat actors are targeting mission-critical SAP enterprise applications unsecured against already patched vulnerabilities, exposing the networks of commercial and government organisations to attacks.

New Cring ransomware hits unpatched Fortinet VPN devices

Date: 08 April 2021

A vulnerability impacting Fortinet VPNs is being exploited by a new human-operated ransomware strain known as Cring to breach and encrypt industrial sector companies' networks.

Alleged North Korean hackers attack a South African freighter company

Date: 09 April 2021

Alleged North Korean-backed Lazarus hacking group used new malware with backdoor capabilities dubbed Vyveva by ESET researchers in targeted attacks against a South African freight logistics company.

Attackers deliver legal threats, IcedID malware via contact forms

Date: 12 April 2021

Threat actors are using legitimate corporate contact forms to send phishing emails that threaten enterprise targets with lawsuits and attempt to infect them with the IcedID info-stealing malware.

Purple Fox EK now exploits a patched vulnerability in Internet Explorer

Date: 16 April 2021

Purple Fox exploit kit now embeds a recent Internet Explorer vulnerability.

Malicious copycats of Zoom and Windscribe personal VPN used in the wild

Date: 16 April 2021

Malicious copies of Zoom and Windscribe VPN have been deployed since December 2020.

REvil/Sodinokibi ransomware group about to target Linux systems

Date: 19 April 2021

The threat actor which operates the REvil/Sodinokibi ransomware has announced that it is making preparations to target Linux systems. Recently, Darkside and Babuk ransomware operators made similar statements in the past.

North Korean hackers adapt web skimming for stealing Bitcoin

Date: 20 April 2021

Researchers from Sansec and Group-IB claim that hackers linked with the North Korean government applied a web skimming technique to steal cryptocurrency in a previously undocumented campaign that started early last year.

Lazarus Group Uses Images to Hide Payload

Date: 20 April 2021

Attacks attributed to the North Korean state-affiliated Lazarus group concealed malicious code within image files to drop its Remote Access Trojan (RAT).

Trend Micro products are being actively exploited in the wild

Date: 22 April 2021

Trend Micro updated a security advisory that was issued last year for a vulnerability, CVE-2020-24557, that relates to Trend Micro Apex One, Apex One as a Service, and OfficeScan Corporate Edition. In the update Trend Micro states that they detected active exploitation attempts of this vulnerability.

Hacking campaign targets FileZen file-sharing network appliances

Date: 26 April 2021

Threat actors are using two vulnerabilities in a popular file-sharing server to breach corporate and government systems and steal sensitive data as part of a global hacking campaign that has already hit a major target in the Japanese Prime Minister’s Cabinet Office.

Passwordstate password manager hacked in supply chain attack

Date: 26 April 2021

ClickStudios, the company behind the Passwordstate password manager, notified customers that attackers compromised the app's update mechanism to deliver malware in a supply-chain attack after breaching its networks.

Flubot malware targets UK android phones via SMS campaign

Date: 28 April 2021

The malware is spreading rapidly through ‘missed package delivery’ SMS texts, prompting urgent scam warnings from mobile carriers.

Babuk Ransomware Gang Targets Washington DC Police

Date: 28 April 2021

On April 26th the Washington DC Police Department confirmed that its computer network had been breached after a ransomware group claimed to have stolen sensitive data, including some about informants, which it threatened to share with local criminal gangs unless police paid a ransom.

RotaJakiro Linux backdoor has been under the radar since 2018

Date: 29 April 2021

Researchers from Qihoo360's Network Security Research Lab (360 Netlab) have discovered a Linux backdoor, nicknamed RotaJakiro. It has remained undetected for many years while harvesting and exfiltrating sensitive information from victims. This malware was not detected by VirusTotal's anti-virus engines, although a template was first uploaded in 2018.

Kaspersky believes they discovered an old malware from the CIA

Date: 29 April 2021

Russian cybersecurity firm Kaspersky announced that it discovered new malware, used in 2014 or 2015, that is believed to have been developed by the US Central Intelligence Agency. The malware was found in a collection of malware samples that its analysts and other security firms received in February 2019.

New ransomware group uses SonicWall zero-day to breach networks

Date: 30 April 2021

A financially motivated threat actor exploited a zero-day bug in Sonicwall SMA 100 Series VPN appliances to deploy new ransomware known as FiveHands on the networks of North American and European targets.

VULNERABILITY MANAGEMENT

April was the month of the zero-day. We published six signals describing previously unknown vulnerabilities being exploited. Some of these zero-days were in security products.

A serious zero-day vulnerability was revealed in the latest version of Pulse Connect Secure VPN product. The vendor published a mitigation with news of a follow-up patch on its way. A file system integrity checking tool was also published to identify any compromised hosts. Active exploitation of vulnerable hosts were detected and is believed to be the work of attackers with strong links to China.

SonicWall Email Security disclosed three zero-days that affected the hosted version of the product as well as the on-premise deployed versions.

Microsoft published security patches for Microsoft Exchange to address more zero-day vulnerabilities. These are a fresh batch of patches and are unrelated to the previous month's excitement around a set of zero-day vulnerabilities known as ProxyLogon.

The number of zero-day vulnerabilities found in web browsers have not decreased. This speaks to the large attack surface looming in these products and how attackers have changed their focus to exploit victims previously thought safe. We continue to report on zero-days found in popular browsers such as Google Chrome.

Legacy QNAP NAS Devices Vulnerable to Zero-Day Attack

Date: 02 April 2021

Some legacy models of QNAP network attached storage devices are vulnerable to remote unauthenticated attacks because of two unpatched vulnerabilities.

Critical vulnerability in the VMware Carbon Black Cloud Workload appliance discovered

Date: 02 April 2021

A flaw in the VMware Carbon Black Cloud Workload appliance has been addressed by VMware.

Cisco fixes bug allowing remote code execution with root privileges

Date: 08 April 2021

Cisco has released security updates to address a pre-authentication remote code execution (RCE) vulnerability affecting SD-WAN vManage Software's user management function.

Vulnerability discovered in time synchronization software from Greyware Automation

Date: 09 April 2021

GRIMM researchers say they discovered a remote code execution (RCE) vulnerability that can allow attackers to hijack the update process of a popular time synchronization software from a company called Greyware Automation.

Google Chrome, Microsoft Edge zero-day vulnerability shared on Twitter

Date: 13 April 2021

A security researcher has dropped a zero-day remote code execution vulnerability on Twitter that works on the current version of Google Chrome and Microsoft Edge.

NAME:WRECK vulnerabilities impact millions of smart and industrial devices.

Date: 13 April 2021

Security researchers have found a new set of vulnerabilities that impact hundreds of millions of servers, smart devices, and industrial equipment.

Adobe Patches Slew of Critical Security Bugs in Bridge, Photoshop

Date: 14 April 2021

The security bugs could open the door for arbitrary code-execution and full takeover of targeted machines.

Microsoft April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days

Date: 14 April 2021

Today is Microsoft's April 2021 Patch Tuesday, and with it comes five zero-day vulnerabilities and more Critical Microsoft Exchange vulnerabilities.

SensePost Discovers Authentication Bypass in Duo 2FA

Date: 20 April 2021

SensePost, the ethical hacking team of Orange Cyberdefense, published a blog post with details on a Duo Two-Factor Authentication bypass they discovered. The flaw could have allowed an attacker to divert the push notification associated with a targeted account to a device under their control instead.

Chinese threat actors leverage a new zero-day in Pulse Secure to target US and European organizations

Date: 21 April 2021

Chinese cyber espionage actors have been using a zero-day vulnerability (CVE-2021-22893) as well as some older, known, vulnerabilities in Pulse Secure VPN to gain access to dozens of government, finance, and defence organisations in the US and Europe.

SonicWall Email Security Targeted with 3 Zero-days

Date: 21 April 2021

Security hardware manufacturer SonicWall is urging customers to patch a set of three zero-day vulnerabilities affecting both its on-premises and hosted Email Security products.

Oracle Releases 390 Security Patches

Date: 21 April 2021

The Critical Patch Update for April 2021 contains several fixes for serious vulnerabilities in popular Oracle products.

Apple Patches Zero-Day MacOS Bug That Can Bypass Anti-Malware Defenses

Date: 28 April 2021

Apple has fixed a zero-day vulnerability in macOS exploited in the wild by Shlayer malware to bypass Apple's security mechanisms.

Google Chrome V8 Bug Allows Remote Code-Execution

Date: 29 April 2021

Google’s Chrome browser has several security vulnerabilities that could pave the way to multiple types of attacks, including a V8 bug that could allow remote code execution (RCE) within a user’s browser.

F5 Big-IP Vulnerable to Security-Bypass Bug

Date: 30 April 2021

F5 Networks’ Big-IP Application Delivery Services appliance contains a Key Distribution Center (KDC) spoofing vulnerability, researchers disclosed – which an attacker could use to get past the security measures that protect sensitive workloads.

NOTEWORTHY

Pierre Fabre is currently under attack by a ransomware group

Date: 01 April 2021

Pierre Fabre is currently under attack by a ransomware group.

22-Year-Old Charged With Hacking Water System and Endangering Lives

Date: 01 April 2021

A 22-year-old man from the U.S. state of Kansas has been indicted on charges that he illegally accessed a public water facility's computer system, jeopardizing the residents' safety and health in the local community.

Over 500 million LinkedIn users data scraped and put for sale

Date: 09 April 2021

An archive containing data scraped from 500 million LinkedIn profiles has been put up for sale on a popular yet low-level hacker forum. 2 million records were leaked for free as a proof-of-concept sample by the post author.

French accounting firm In Extenso targeted by a ransomware attack

Date: 16 April 2021

French accounting firm In Extenso targeted by a ransomware attack.

The United States sanctions Russia for the Solarwinds hack

Date: 16 April 2021

The United States formally attributed Solarwinds hack to Russia and issued sanctions against Russian companies alleged to help Russian government conducting malicious cyber activities.

Major BGP leak disrupts thousands of networks globally

Date: 19 April 2021

A large Border Gateway Protocol (BGP) routing leak that occurred last night disrupted the connectivity for thousands of major networks and websites around the world. Although the BGP routing leak occurred in Vodafone's autonomous network (AS55410) based in India, it has impacted U.S. companies, including Google, according to sources.

Darkside Ransomware Group Expands Extortion Tactics

Date: 23 April 2021

In a message posted on their dark web portal, the Darkside crew said it is willing to notify crooked market traders in advance so they can short a company’s stock price before they list its name on their website as a victim.

Federated Learning of Cohorts

Date: 28 April 2021

Federated Learning of Cohorts or more commonly referred to as FLoC is a proposal by Google to enable third-parties to serve targeted content or perform analytics by removing the need for third-party cookies or similar tracking methods.