CYJAX

Digital Intelligence
Securing the Future

Cyjax Service Update [December 2020]

CLIENT CONFIDENTIAL

Dear Clients,

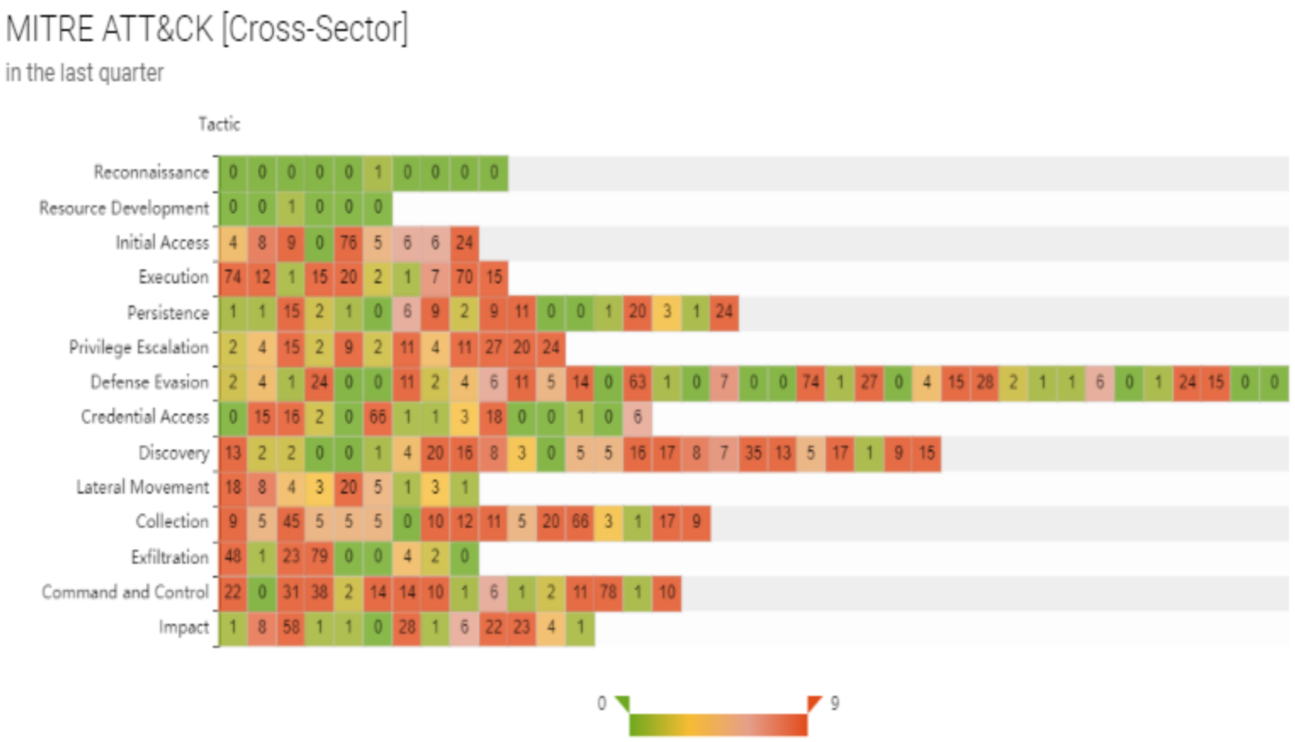
We have made some exciting new enhancements to our service over the past several months and wanted to outline them to you. Firstly, however, we hope that you are all doing well during what has been a difficult time, made no easier by the associated malicious cyber activity. Looking ahead to 2021, we will maintain our efforts to ensure you are able to make informed business decisions and better protect your organisation.

So what's new? Our attack surface and domain monitoring services continue to improve, and we have now rolled out a new global search facility. You will also notice that we have tweaked our IOC search facility which will allow you to check against Cyjax incident reports, as well as various reputation lists. Finally, we are offering more compelling ways to visualise our data along with even more pre-built dashboards that will aid in your operations.

New Cyjax Platform Technology

MITRE ATT&CK Heat Maps

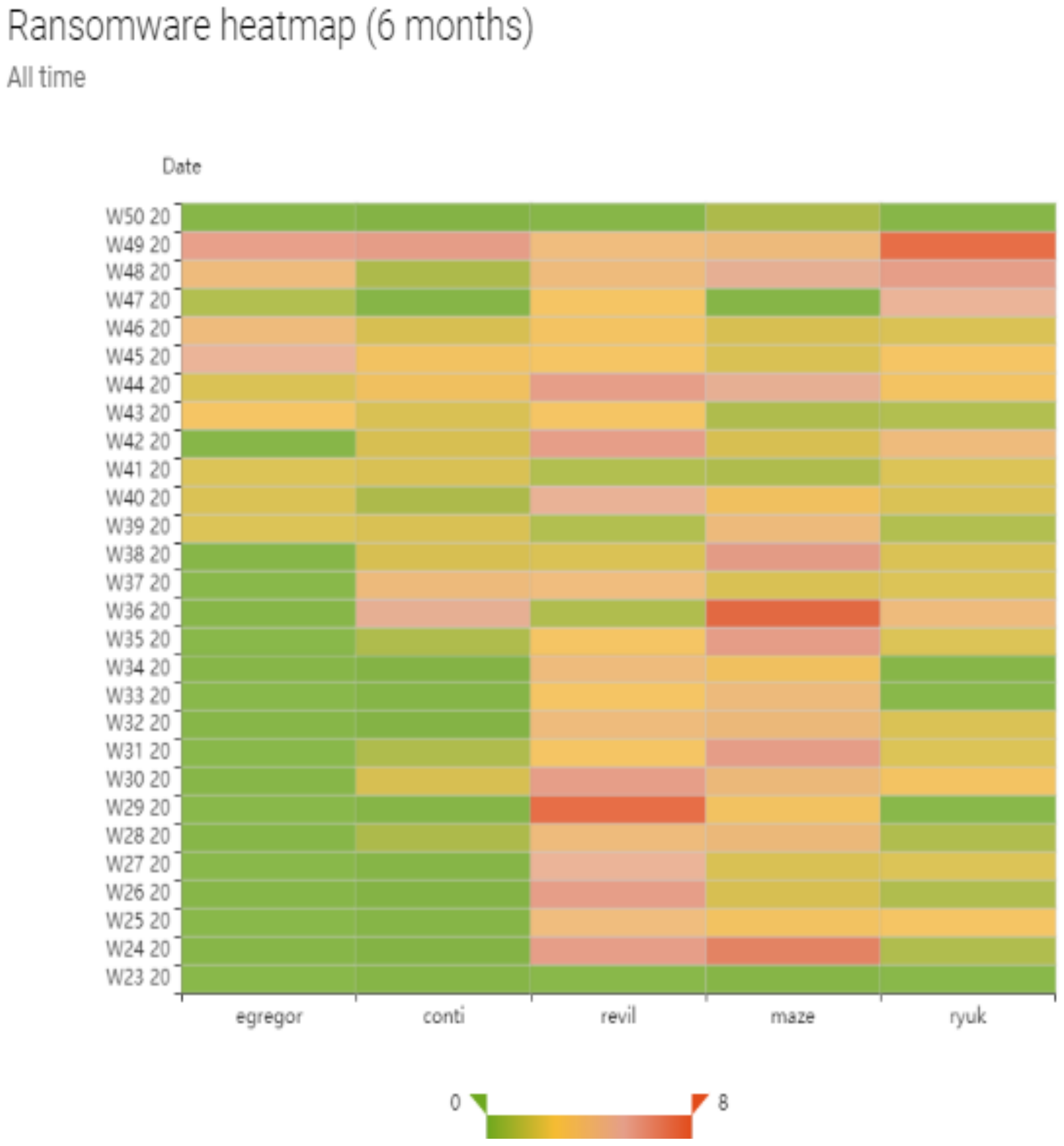
We have been mapping to the MITRE ATT&CK framework for most of 2020. However, we wondered, what if you could visualise ATT&CK behaviour from a higher level using a heatmap and run that against a specific vertical or threat actor? As such, we have delivered the ability to do just that using our brand new MITRE ATT&CK heatmap widgets:



To create a MITRE ATT&CK heatmap, please refer to the documentation here.

Heat map widgets

We have also rolled out a heatmap widget which will allow you to visualise other types of data over a given period of time. For example, if you wanted to visualise ransomware over the past six months, you can do that quite effectively, as shown below:



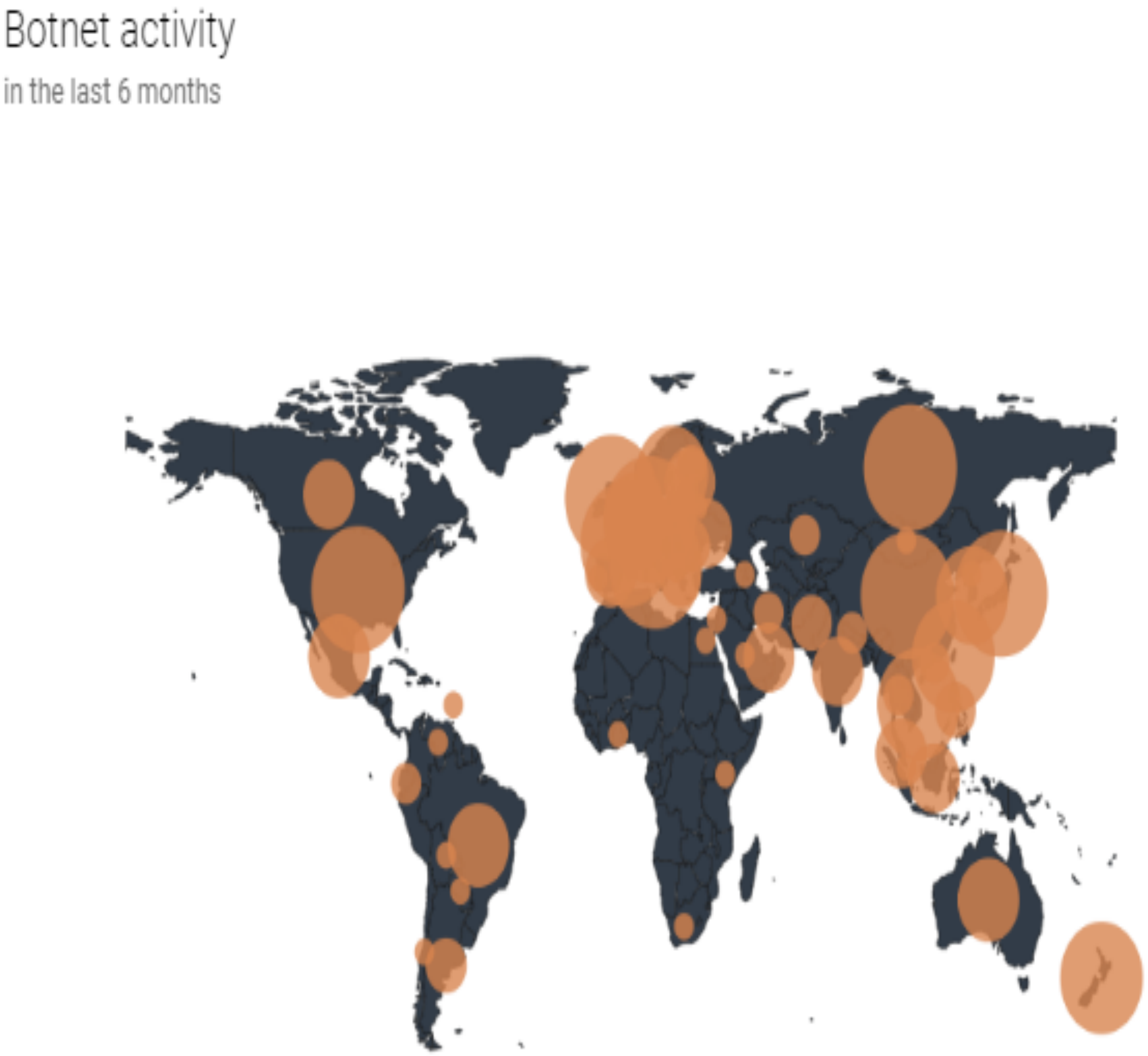
Ransomware heatmap (6 months)

All time

To create a Heatmap widget, please refer to the documentation here.

Global maps

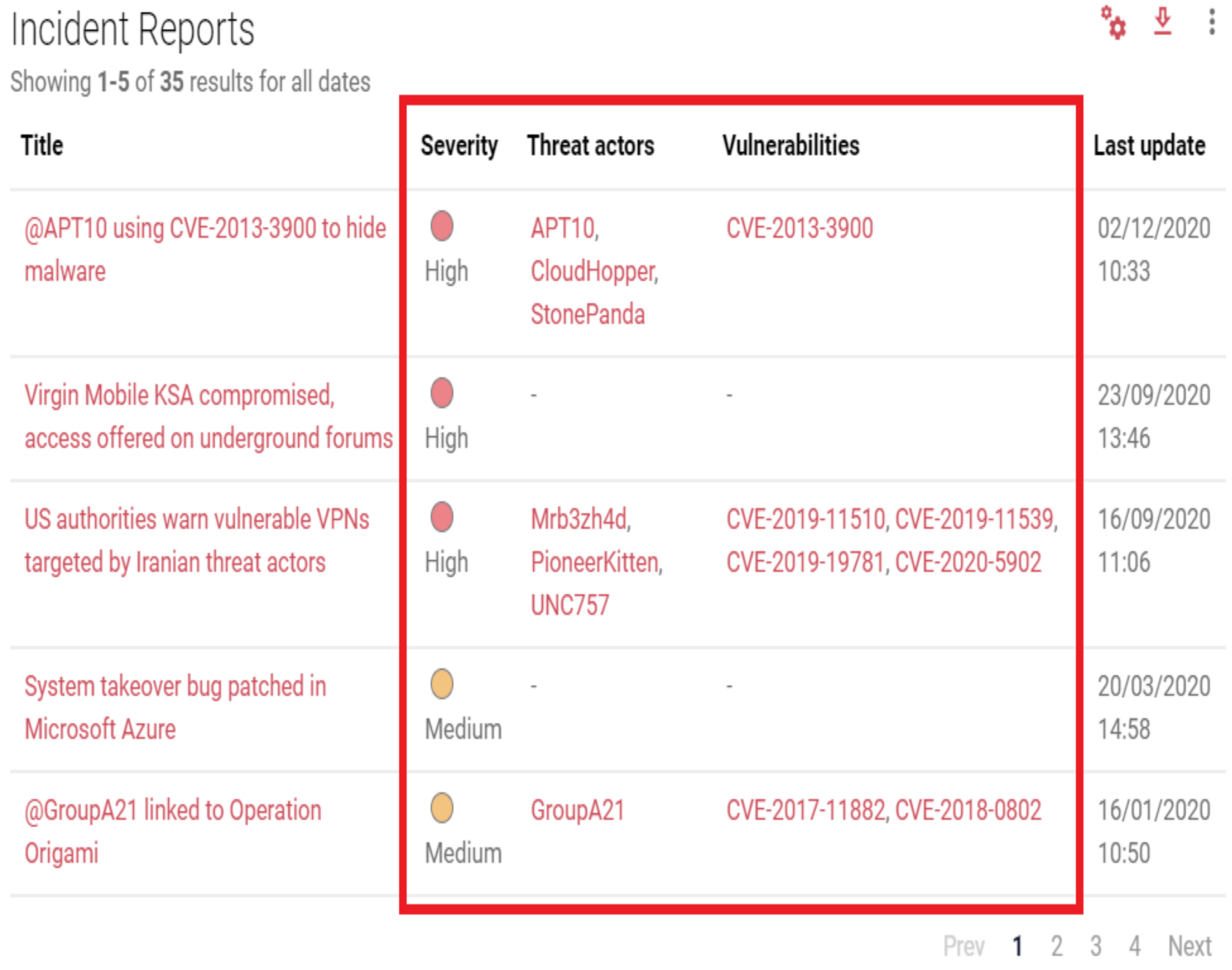
You can now visualise content specific to incident reports on a global map widget, as follows:



To create a Global map widget, please refer to the documentation here.

Enhancements to IR widgets - severity scores, vulnerabilities, threat actors

We have made some enhancements to our Incident Report widgets - you can now visualise additional information in table widgets, including severity scores, vulnerabilities, and threat actors associated with any particular incident.



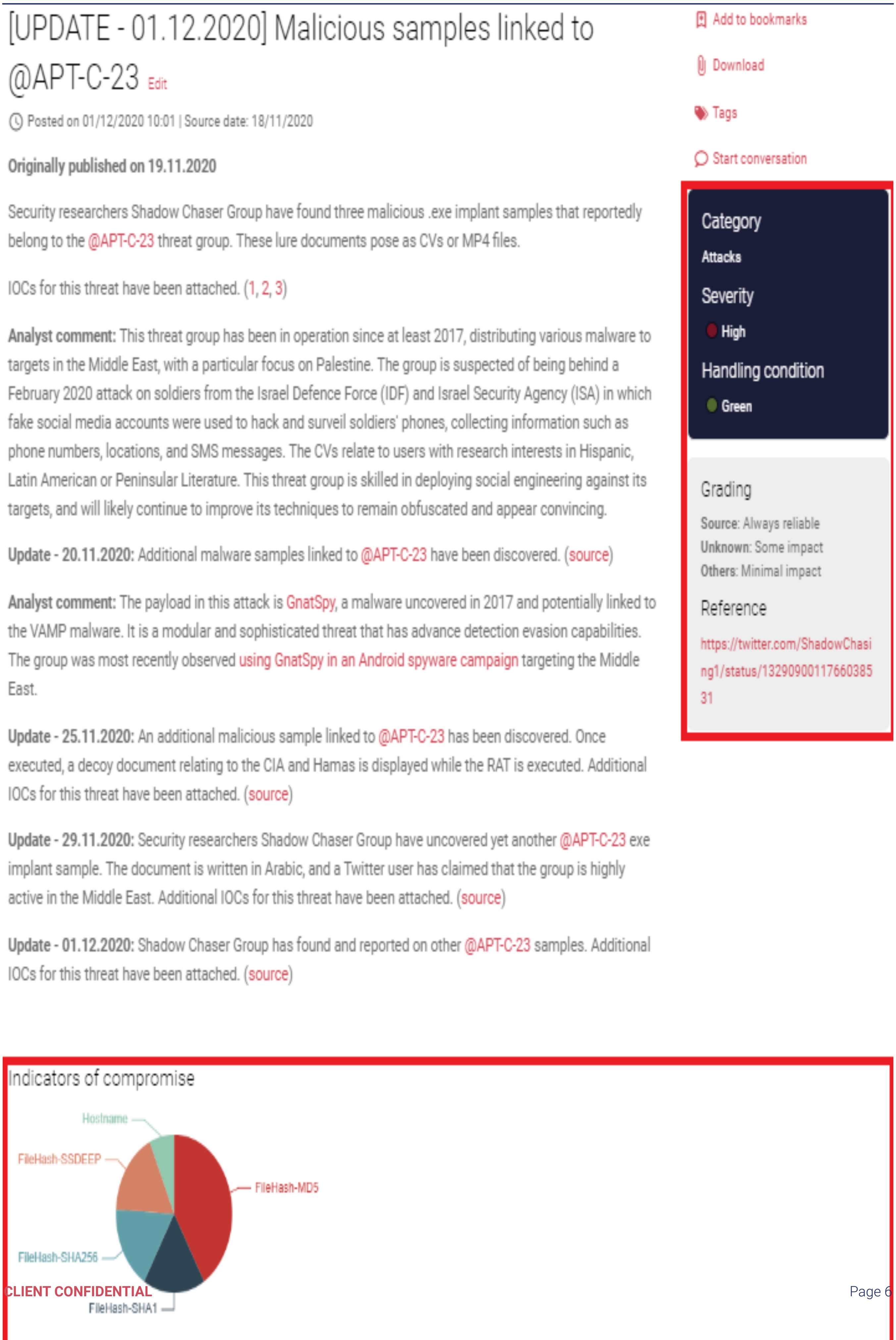
Incident Reports

Showing **1-5** of **35** results for all dates

Title	Severity	Threat actors	Vulnerabilities	Last update
@APT10 using CVE-2013-3900 to hide malware	● High	APT10, CloudHopper, StonePanda	CVE-2013-3900	02/12/2020 10:33
Virgin Mobile KSA compromised, access offered on underground forums	● High	-	-	23/09/2020 13:46
US authorities warn vulnerable VPNs targeted by Iranian threat actors	● High	Mrb3zh4d, PioneerKitten, UNC757	CVE-2019-11510, CVE-2019-11539, CVE-2019-19781, CVE-2020-5902	16/09/2020 11:06
System takeover bug patched in Microsoft Azure	● Medium	-	-	20/03/2020 14:58
@GroupA21 linked to Operation Origami	● Medium	GroupA21	CVE-2017-11882, CVE-2018-0802	16/01/2020 10:50

Enhanced and redesigned incident reports

We have made some changes to the design of our incident reports. You will notice a clearer aesthetic to the reports that we hope will enable you to better visualise the information contained within them.



[UPDATE - 01.12.2020] Malicious samples linked to @APT-C-23

Posted on 01/12/2020 10:01 | Source date: 18/11/2020

Originally published on 19.11.2020

Security researchers Shadow Chaser Group have found three malicious .exe implant samples that reportedly belong to the @APT-C-23 threat group. These lure documents pose as CVs or MP4 files.

IOCs for this threat have been attached. (1, 2, 3)

Analyst comment: This threat group has been in operation since at least 2017, distributing various malware to targets in the Middle East, with a particular focus on Palestine. The group is suspected of being behind a February 2020 attack on soldiers from the Israel Defence Force (IDF) and Israel Security Agency (ISA) in which fake social media accounts were used to hack and surveil soldiers' phones, collecting information such as phone numbers, locations, and SMS messages. The CVs relate to users with research interests in Hispanic, Latin American or Peninsular Literature. This threat group is skilled in deploying social engineering against its targets, and will likely continue to improve its techniques to remain obfuscated and appear convincing.

Update - 20.11.2020: Additional malware samples linked to @APT-C-23 have been discovered. (source)

Analyst comment: The payload in this attack is GnatSpy, a malware uncovered in 2017 and potentially linked to the VAMP malware. It is a modular and sophisticated threat that has advance detection evasion capabilities. The group was most recently observed using GnatSpy in an Android spyware campaign targeting the Middle East.

Update - 25.11.2020: An additional malicious sample linked to @APT-C-23 has been discovered. Once executed, a decoy document relating to the CIA and Hamas is displayed while the RAT is executed. Additional IOCs for this threat have been attached. (source)

Update - 29.11.2020: Security researchers Shadow Chaser Group have uncovered yet another @APT-C-23 exe implant sample. The document is written in Arabic, and a Twitter user has claimed that the group is highly active in the Middle East. Additional IOCs for this threat have been attached. (source)

Update - 01.12.2020: Shadow Chaser Group has found and reported on other @APT-C-23 samples. Additional IOCs for this threat have been attached. (source)

Category

Attacks

Severity

● High

Handling condition

● Green

Grading

Source: Always reliable

Unknown: Some impact

Others: Minimal impact

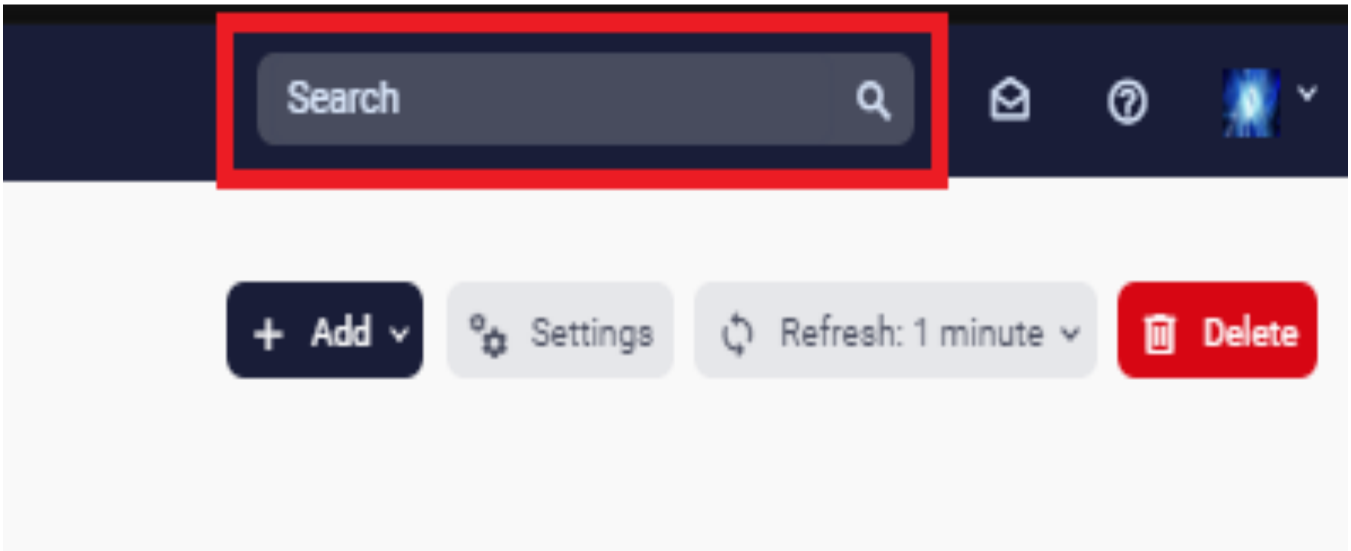
Reference

https://twitter.com/ShadowChasing1/status/1329090011766038531

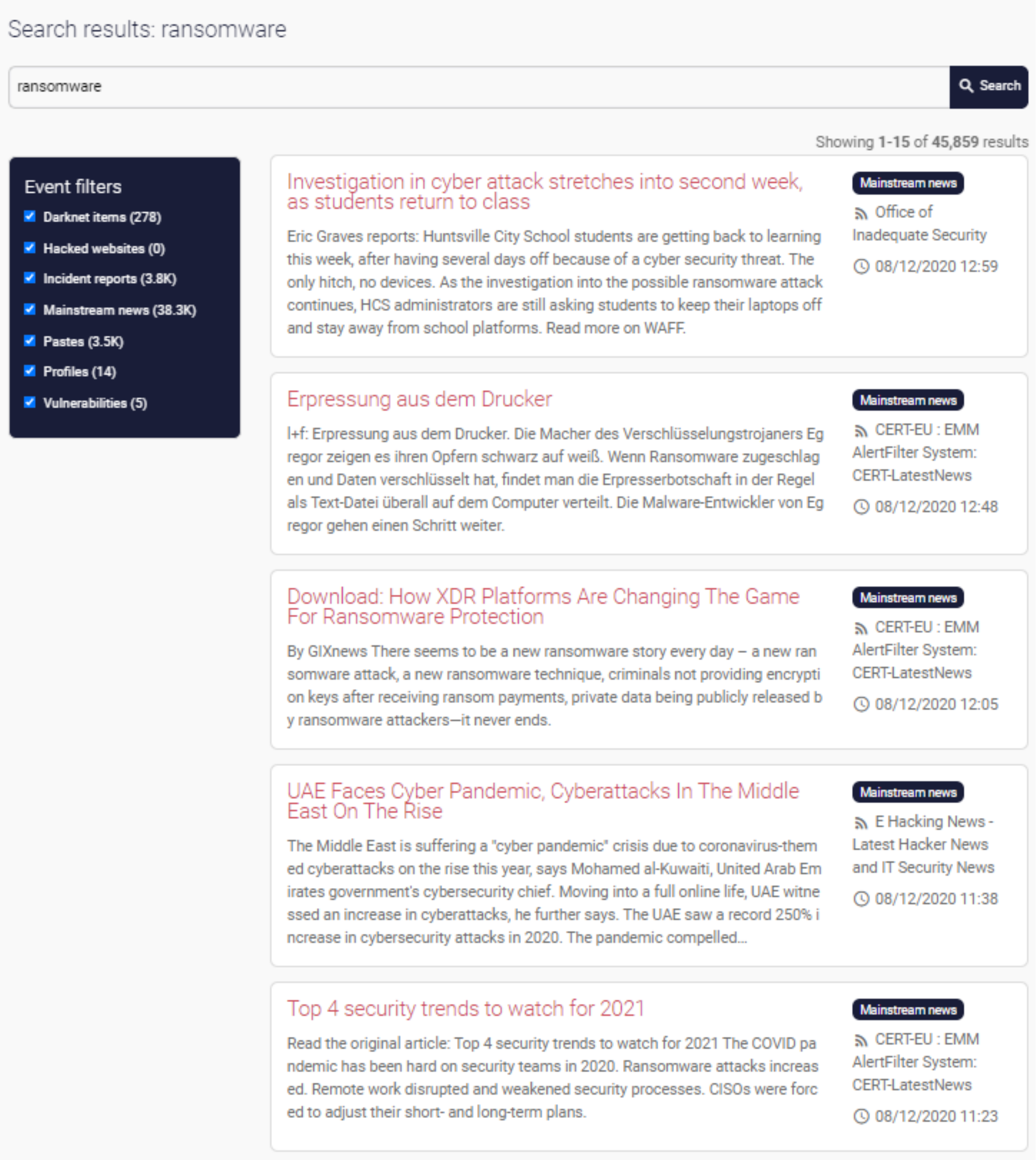
Indicators of compromise

Global search

We are extremely happy to introduce our global search functionality to the platform. You will now be able to effectively search across the various data stores and pull back results:



If we add "ransomware" as a search term, you can expect the results below, filtering across all our data stores and then displayed as shown below. You can then untick the box next to the specific data store that you don't want to visualise in the results.



Search results: ransomware

Showing **1-15** of **45,859** results

Event filters

- ☑ Darknet items (278)
- ☑ Hacked websites (0)
- ☑ Incident reports (3.8K)
- ☑ Mainstream news (38.3K)
- ☑ Pastes (3.5K)
- ☑ Profiles (14)
- ☑ Vulnerabilities (5)

Investigation in cyber attack stretches into second week, as students return to class

Eric Graves reports: Huntsville City School students are getting back to learning this week, after having several days off because of a cyber security threat. The only hitch, no devices. As the investigation into the possible ransomware attack continues, HCS administrators are still asking students to keep their laptops off and stay away from school platforms. Read more on WAFF.

Mainstream news
Office of Inadequate Security
08/12/2020 12:59

Erpressung aus dem Drucker

I+f: Erpressung aus dem Drucker. Die Macher des Verschlüsselungstrojaners Eg regor zeigen es ihren Opfern schwarz auf weiß. Wenn Ransomware zugeschlag en und Daten verschlüsselt hat, findet man die Erpresserbotschaft in der Regel als Text-Datei überall auf dem Computer verteilt. Die Malware-Entwickler von Eg regor gehen einen Schritt weiter.

Mainstream news
CERT-EU : EMM AlertFilter System: CERT-LatestNews
08/12/2020 12:48

Download: How XDR Platforms Are Changing The Game For Ransomware Protection

By GIXnews There seems to be a new ransomware story every day – a new ran somware attack, a new ransomware technique, criminals not providing encrypti on keys after receiving ransom payments, private data being publicly released b y ransomware attackers—it never ends.

Mainstream news
CERT-EU : EMM AlertFilter System: CERT-LatestNews
08/12/2020 12:05

UAE Faces Cyber Pandemic, Cyberattacks In The Middle East On The Rise

The Middle East is suffering a "cyber pandemic" crisis due to coronavirus-them ed cyberattacks on the rise this year, says Mohamed al-Kuwaiti, United Arab Em irates government's cybersecurity chief. Moving into a full online life, UAE witne ssed an increase in cyberattacks, he further says. The UAE saw a record 250% i ncrease in cybersecurity attacks in 2020. The pandemic compelled...

Mainstream news
E Hacking News - Latest Hacker News and IT Security News
08/12/2020 11:38

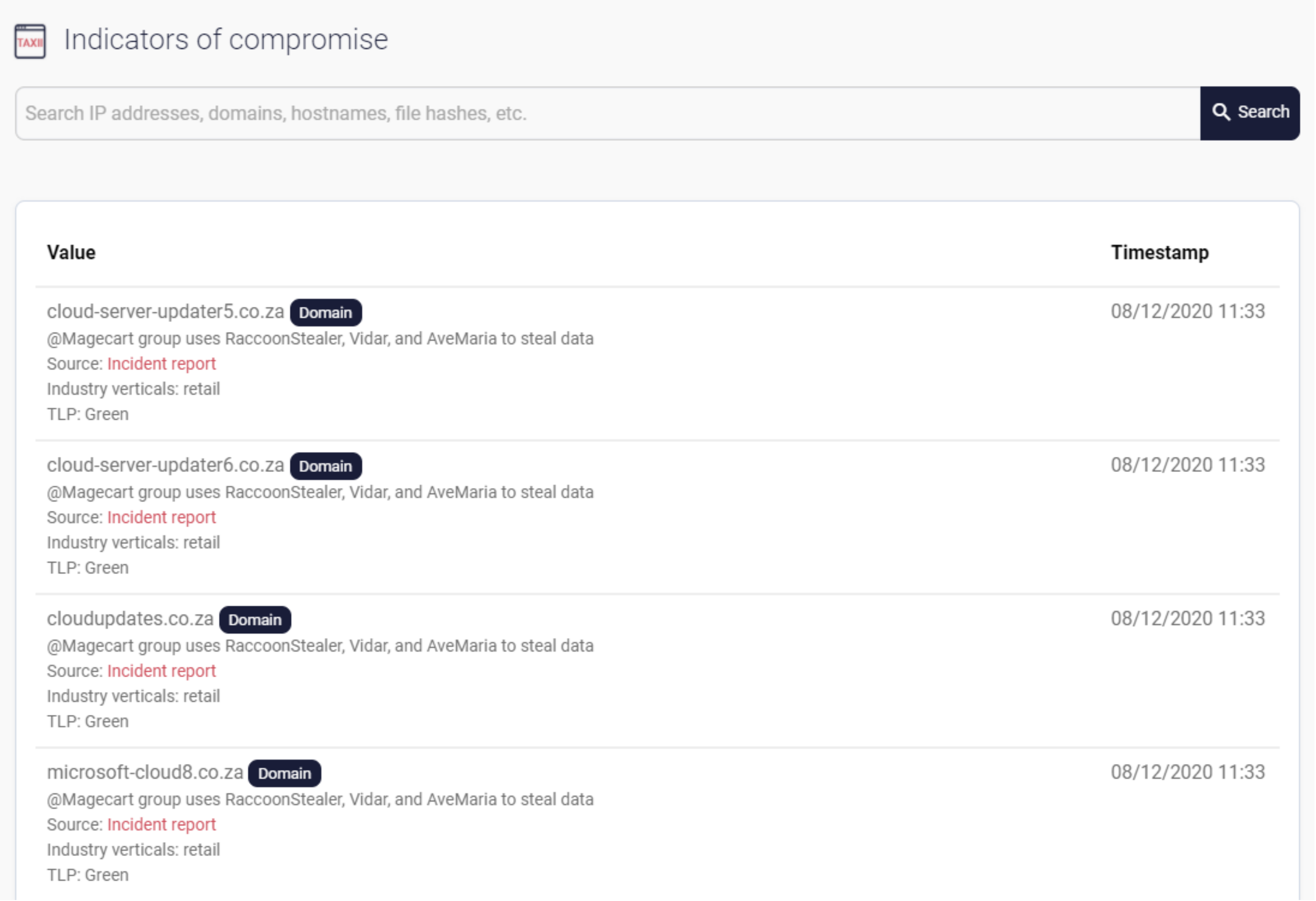
Top 4 security trends to watch for 2021

Read the original article: Top 4 security trends to watch for 2021 The COVID pa ndemic has been hard on security teams in 2020. Ransomware attacks increas ed. Remote work disrupted and weakened security processes. CISOs were forc ed to adjust their short- and long-term plans.

Mainstream news
CERT-EU : EMM AlertFilter System: CERT-LatestNews
08/12/2020 11:23

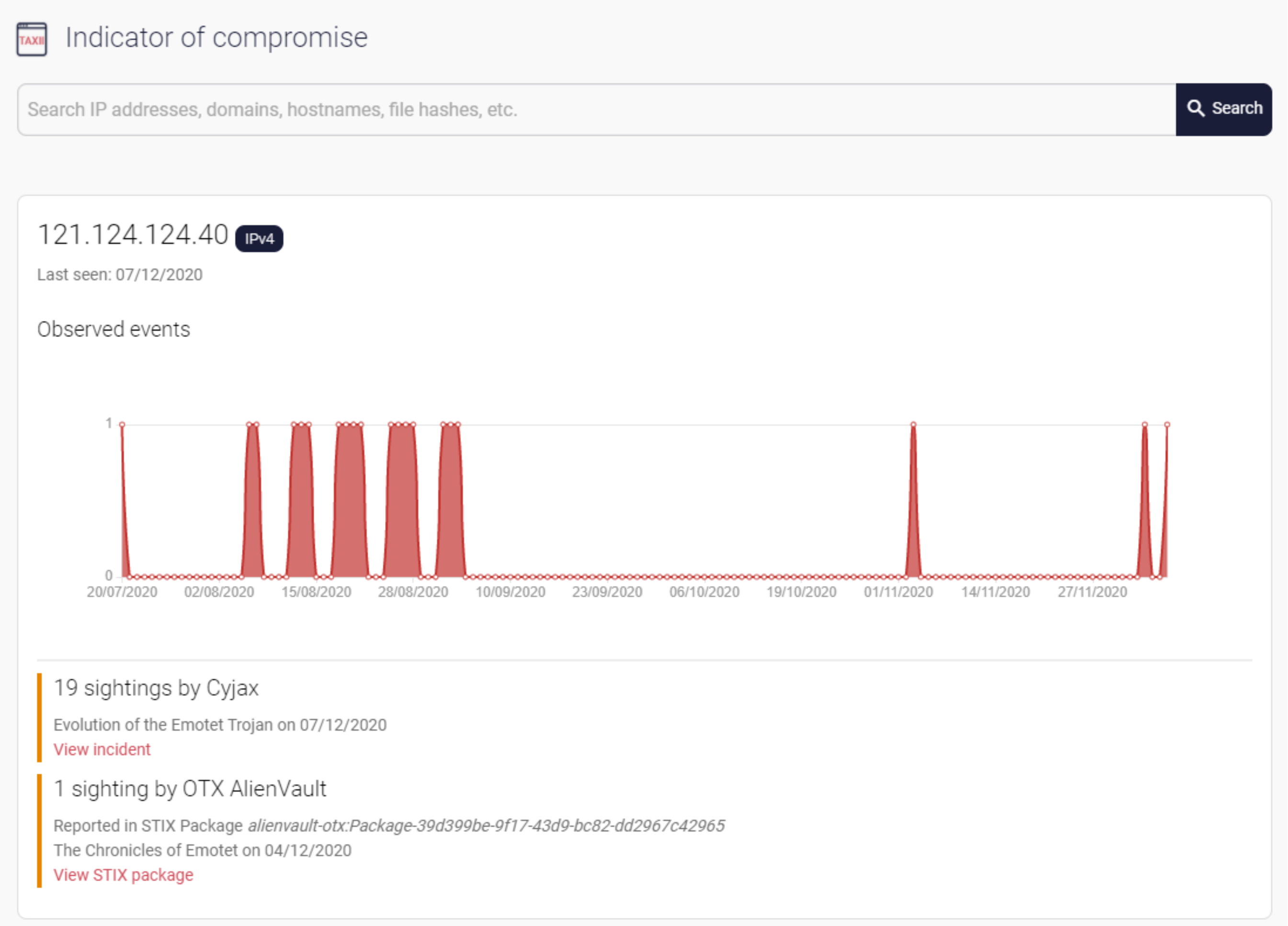
IOC front-end

We have rolled out a new Indicators of Compromise search facility. Explore indicators across the range of our reports, various reputation lists, and threat feeds, including DHS Automated Indicator Sharing and Open Threat Exchange.



Value	Timestamp
cloud-server-updater5.co.za Domain @Magecart group uses RaccoonStealer, Vidar, and AveMaria to steal data Source: Incident report Industry verticals: retail TLP: Green	08/12/2020 11:33
cloud-server-updater6.co.za Domain @Magecart group uses RaccoonStealer, Vidar, and AveMaria to steal data Source: Incident report Industry verticals: retail TLP: Green	08/12/2020 11:33
cloudupdates.co.za Domain @Magecart group uses RaccoonStealer, Vidar, and AveMaria to steal data Source: Incident report Industry verticals: retail TLP: Green	08/12/2020 11:33
microsoft-cloud8.co.za Domain @Magecart group uses RaccoonStealer, Vidar, and AveMaria to steal data Source: Incident report Industry verticals: retail TLP: Green	08/12/2020 11:33

Further, you will be able to see how often each indicator occurs across our sources. For example, if we run an IP address as follows, you can see how many the number of sightings by our various sources:



Indicator of compromise

121.124.124.40 IPv4

Last seen: 07/12/2020

Observed events

19 sightings by Cyjax

Evolution of the Emotet Trojan on 07/12/2020

View incident

1 sighting by OTX AlienVault

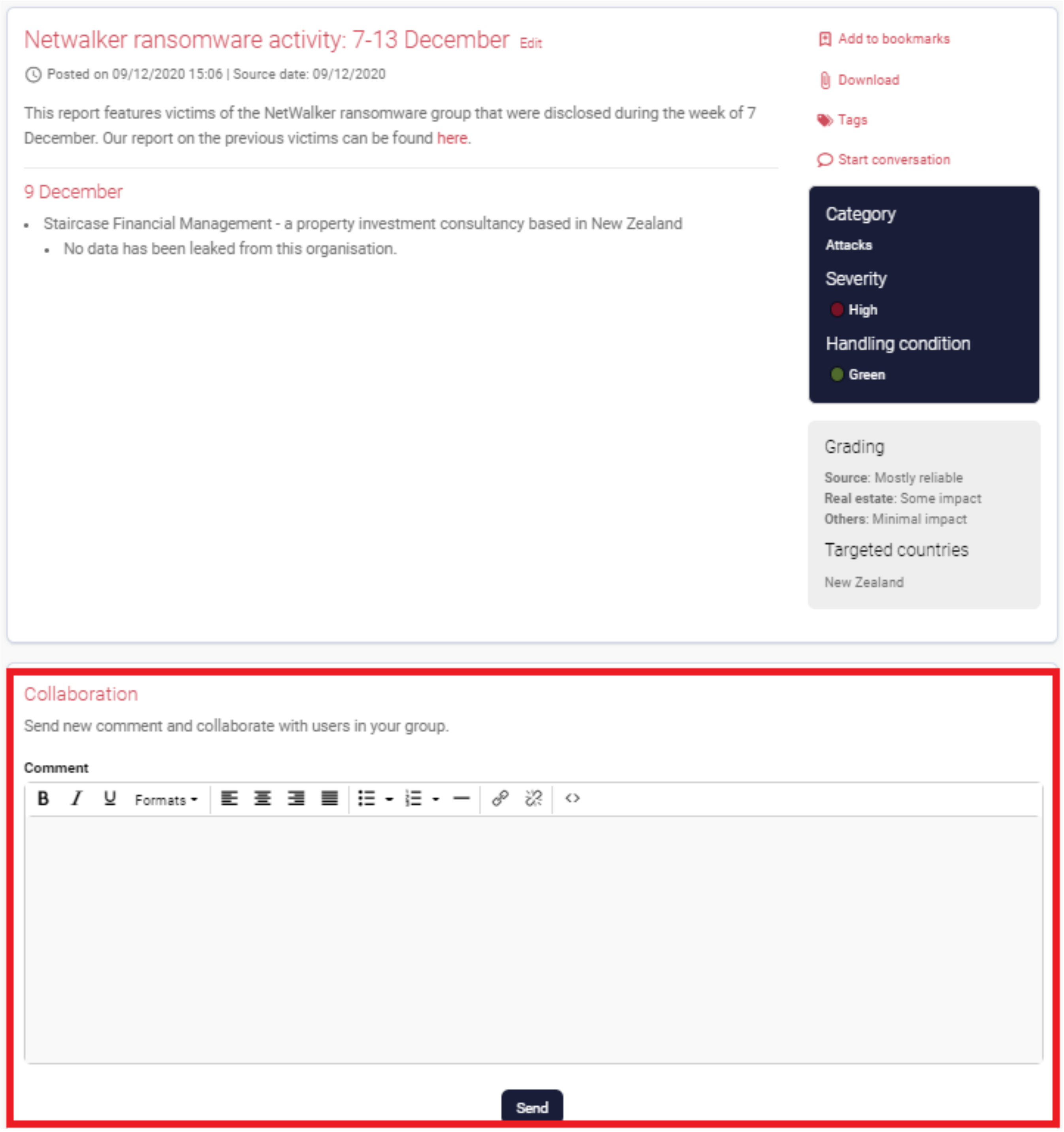
Reported in STIX Package *alienvault-otx:Package-39d399be-9f17-43d9-bc82-dd2967c42965*

The Chronicles of Emotet on 04/12/2020

View STIX package

Brand new collaboration feature

This will allow you to make comments on reports and share with them with other members of your group. The group collaboration feature is available both for Incident Reports and Live Intelligence. These comments will only exist within your own group - they will not be shared with Cyjax or any other group we control. If you need to collaborate with our team, you should use the 'Start conversation' link located just above the blue box in the top-righthand corner of an incident report.



Netwalker ransomware activity: 7-13 December

Posted on 09/12/2020 15:06 | Source date: 09/12/2020

This report features victims of the NetWalker ransomware group that were disclosed during the week of 7 December. Our report on the previous victims can be found here.

9 December

- Staircase Financial Management - a property investment consultancy based in New Zealand
  - No data has been leaked from this organisation.

Category
Attacks

Severity
● High

Handling condition
● Green

Grading
Source: Mostly reliable
Real estate: Some impact
Others: Minimal impact

Targeted countries
New Zealand

Collaboration

Send new comment and collaborate with users in your group.

Comment

Public dashboards

We continue to develop our public dashboards with a view to helping you better operationalise the threat information. These dashboards may be copied and then further customised according to your exact requirements. The following dashboards are available:

- Malware monitoring dashboard
- Hacking and carding forums dashboard
- Vulnerabilities and exploit dashboard

- News brief dashboard
- COVID-19 monitoring dashboard
- Fraudulent activity dashboard
- APT/State-sponsored/high-risk
- Reddit & 4Chan dashboard
- Single pane dashboard
- Weekly Threat Landscape dashboard
- MITRE ATT&CK dashboard

Platform documentation

We have overhauled all of our platform documentation, including the Help Hub and the Developer Guide. You will find everything you need to know about the Cyjax platform and how to make use of the APIs, obtain your personal access tokens and any information around integrations we offer.

Help Hub: https://cymon.co/help

Developer Guide: https://cymon.co/development

HaveIBeenPwned

The HIBP integration is slated for release in February 2021.

We have been reaching out to all clients ahead of this update to inform you of the changes to the service. However, if you have any issues or you would like a further session to clarify further anything contained in this update, please get in touch.

Thank you for your continued trust in Cyjax.

Serge Palladino (sp@cyjax.com)

STATEMENT OF CONFIDENTIALITY

This document contains confidential trade secrets and proprietary information of Cyjax Limited. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organisation without express written permission from Cyjax Limited. By accepting this document, the recipient affirms that they will comply with these expectations.

Cyjax Limited, Registered in England and Wales no 08302026.
Registered Office Suite 53 Peek House, 20 Eastcheap, London EC3M 1EB.
United Kingdom.