

How to get ahead of the storm by leveraging intelligence.

Simen Van der Perre, Strategic Advisor







Challenge

**Sophisticated threats,
complex solutions, limited
resources and expertise.**

How to...

... find signals in
the noise & stay
ahead of threats?



... make best use
of security
technology?




... focus on real
priorities?



... be agile and
adaptive?



intelligence noun

in·tel·li·gence | \ in- 'te-lə-jən(t)s  \

1. **information** concerning an enemy or possible enemy or an area
2. the **ability** to learn or understand or to deal with new or trying situations



What are we generally buying?

TREND: COMPLEX INDICATORS ARE MORE LIKELY TO DETECT UNKNOWN APT-RELATED ACTIVITY

Detecting the APT is incredibly difficult and many organizations are not prepared to effectively identify that they have been compromised. In most cases, initial notification of an APT intrusion originated from a third-party, primarily law enforcement. The primary reason organizations fail to identify the APT is that most of their security devices examine inbound traffic at the perimeter. Most organizations rely solely on anti-virus solutions to provide host-based monitoring. In addition, implementing the ability to monitor internal communications on a network is costly and challenging. In both instances, being able to respond quickly and to deploy APT indicators is difficult, as organizations' security arsenals are not configured to monitor using this methodology.

Host- and network-based signatures used to detect malicious activity have previously consisted of data like MD5, file size, file name, and service name, etc. Although useful, the lifespan of these type of signatures is often short because attackers can routinely modify their malware to avoid detection. Although those signatures will periodically work to identify attacker activity, MANDIANT has found greater success in adapting specific signatures into what are known as **Indicators of Compromise** ("IOC" or "indicators").

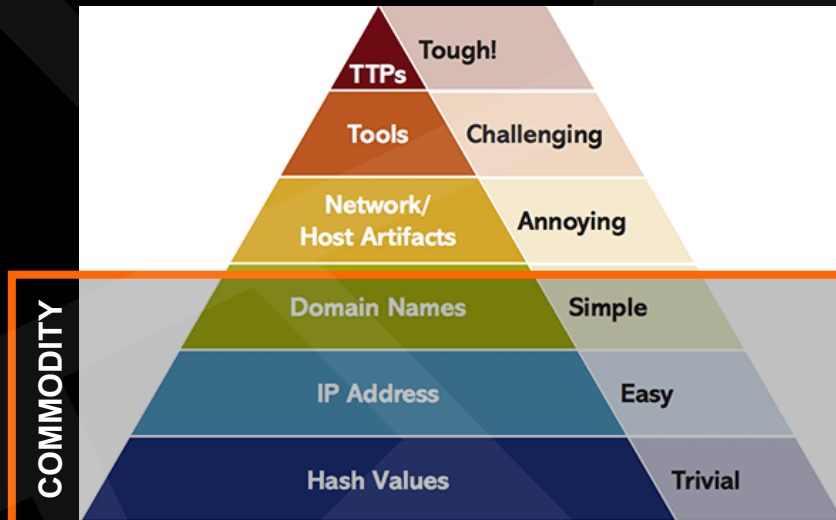
These indicators not only look for specific file and system information, but also use logical statements that characterize malicious activity in greater detail.

MANDIANT has determined that the majority of APT custom-developed tools typically contain code segments from other, similarly developed malware. The code segments could also be upgrades to previously identified malware. Indicators derived from this information remain fairly consistent between the various malware and their subsequent upgrades. Victims are more likely to detect APT-related activity using code segments when it is possible new APT malware might be used. In many cases, previously unidentified malware and backdoors were identified through the use of these indicators in both network traffic and host-based information.

The combination of both host- and network-based indicators continues to be the most reliable way to identify APT-related malware on a network. In two separate investigations, network-based information from a generic packed file transfer revealed suspect malicious activity. Upon further research, the file transfer was identified as malicious activity that was then immediately validated through the use of host-based indicators and forensic analysis.



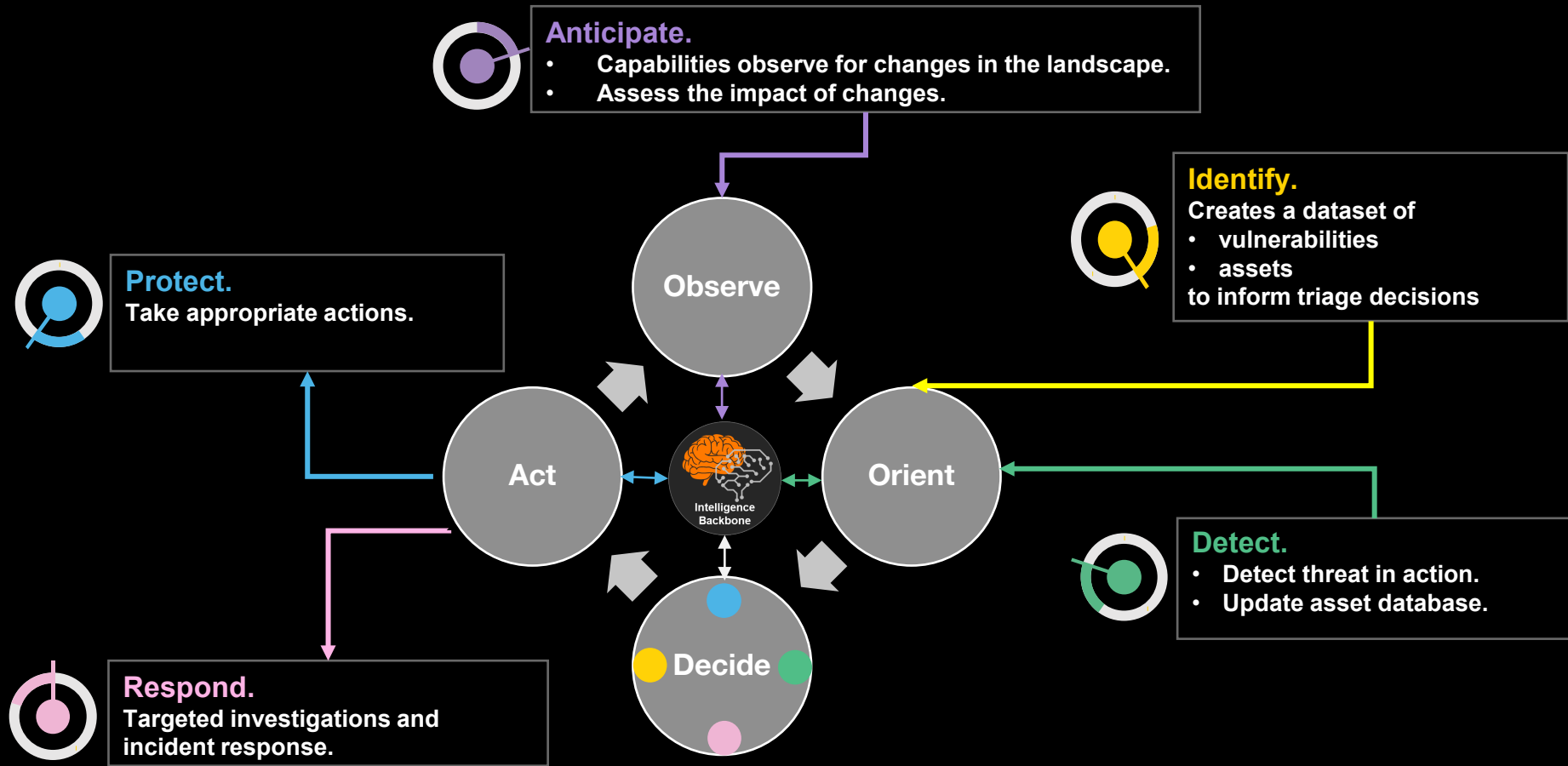
The first documented appearance of the term indicators of compromise, or IOCs, in the modern context is from the first Mandiant M-Trends report, published on 25 Jan 2010.



Source: David J. Bianco, personal blog

Being intelligent

Being intelligent, vs having intelligence



Intelligent machines

Applying basic ML to identify trends

- Commercial
- Free to public
- Service add-on
- Part of customer briefings

CLIMATE



State of the Threat



Monthly Intelligence Report



Navigator Intelligence Report



Stories about Stories

SHORT TERM



World Watch

LONG TERM



Threat Intelligence Report



Managed Vulnerability Intelligence



Managed Threat Intelligence



Strategic



Tactical



Operational

WEATHER

World watch



Complimentary access to World Watch until 31st May 2022

We are pleased to offer all customers complimentary access to [World Watch](#) via the portal, until the end of May.

This cyber-threat advisory service provides qualified, actionable threat intelligence from our CERT to help you keep your organization secure.

After the trial period, non-subscribers of World Watch will solely be able to access a summary advisory.

If you are not currently a subscriber and wish to keep receiving detailed advisories via the portal, please contact your Service Delivery Manager to sign up for World Watch.

• There have been 546 new signals since your last login

Reference

SIG-

Search

Search

Filter

Reset

Signals

Flagged



Analytics

Reference	Summary
SIG-489424	Updated - Emotet is experimenting more deployment techniques using Windows shortcuts
SIG-602371	Updated - New TTPs and findings on TA410's connection to Chinese APT10
SIG-554848	Updated - Microsoft and Kaspersky release new insights on the full-scale of cyberattacks in Ukraine
SIG-607075	New set of privilege escalation vulnerabilities dubbed Nimbuspin in a Linux component
SIG-607019	New Black Basta ransomware operation targets German, French and US-based companies
SIG-606731	Trial in the US sheds light on India-based Dark Basin hack-for-hire group.
SIG-593234	Updated - Leaked Telegram chats reveal evidence on LapouS and their victims
SIG-512974	Updated - New GoldBackdoor malware leveraged by North Korea's APT37 for counterintelligence

New Black Basta ransomware operation targets German, French and US-based companies

Main category

Threat

Urgency

Low

Updated

27/04/2022

Our reference

Signal: SIG-607019

What you will hear

New Black Basta ransomware operation targets German, French and US-based companies.

What it means

Last weekend, the new ransomware gang known as Black Basta claimed responsibility for the attack on the American Dental Association, a dentist and oral hygiene advocacy association providing training, workshops, and courses to its 175,000 members. Quite rapidly after the claim, Black Basta started leaking data stolen during the attack in their own leak site. While the group initially claimed to have leaked approximately 2.8 GB of data (allegedly 30% of the data stolen), the leaks are currently no longer available and ADA's name is not featured anymore on the website. Looking deeper into the ransomware, encrypted files are appended with the extension: .basta while the ransom note is called: readme.txt. According to security analyst @Amigo_A_ on Twitter, the ransomware also used Gh0st RAT, a widely used tool capable of infiltrating targeted Windows systems. During the infection chain, Black Basta operators replaced the desktop wallpaper with its own image. They also rebooted the computer using a shutdown function with attributes (shutdown -r -f -t 0), deleted shadow copies of files, disabled the Windows recovery and repair functions at the boot stage, booted the PC in safe mode and finally changed the appearance of encrypted files using a prepared ico file. Few information concerning initial access was provided so far. On Twitter, security researchers from Kela identified that the Black Basta group had recently declared themselves ready to buy network access on cybercrime forums and deposited 1 Bitcoin on Exploit. We attribute a risk-level of 2 to this alert as this is a novel and developing threat targeting European companies. We expect to see more attacks emanating from this ransomware operation in the coming months.

What we are doing

We will continue to track, analyse, and share information relating to active threats.

What you should do

We advise you check out our Yara Rule created by our Reverse team in the Appendices. It should however be noted that only one indicator connected to the ransomware has been disclosed on VT yet, meaning this Yara Rule might not suffice to detect the malware if the latter uses other files to infect new victims.

Read more

<https://id-ransomware.blogspot.com/2022/04/blackbasta-ransomware.html>

Indicators of compromise

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6ba6b094b0a52b0aa

Updates

Download PDF



PDF link only supported if using Google Chrome, Mozilla Firefox or Internet Explorer web browsers and popups are enabled for this site.

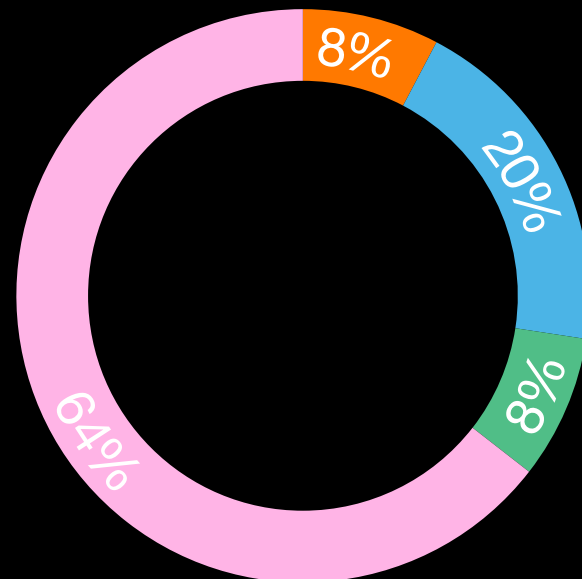
Close

Actionable advisories

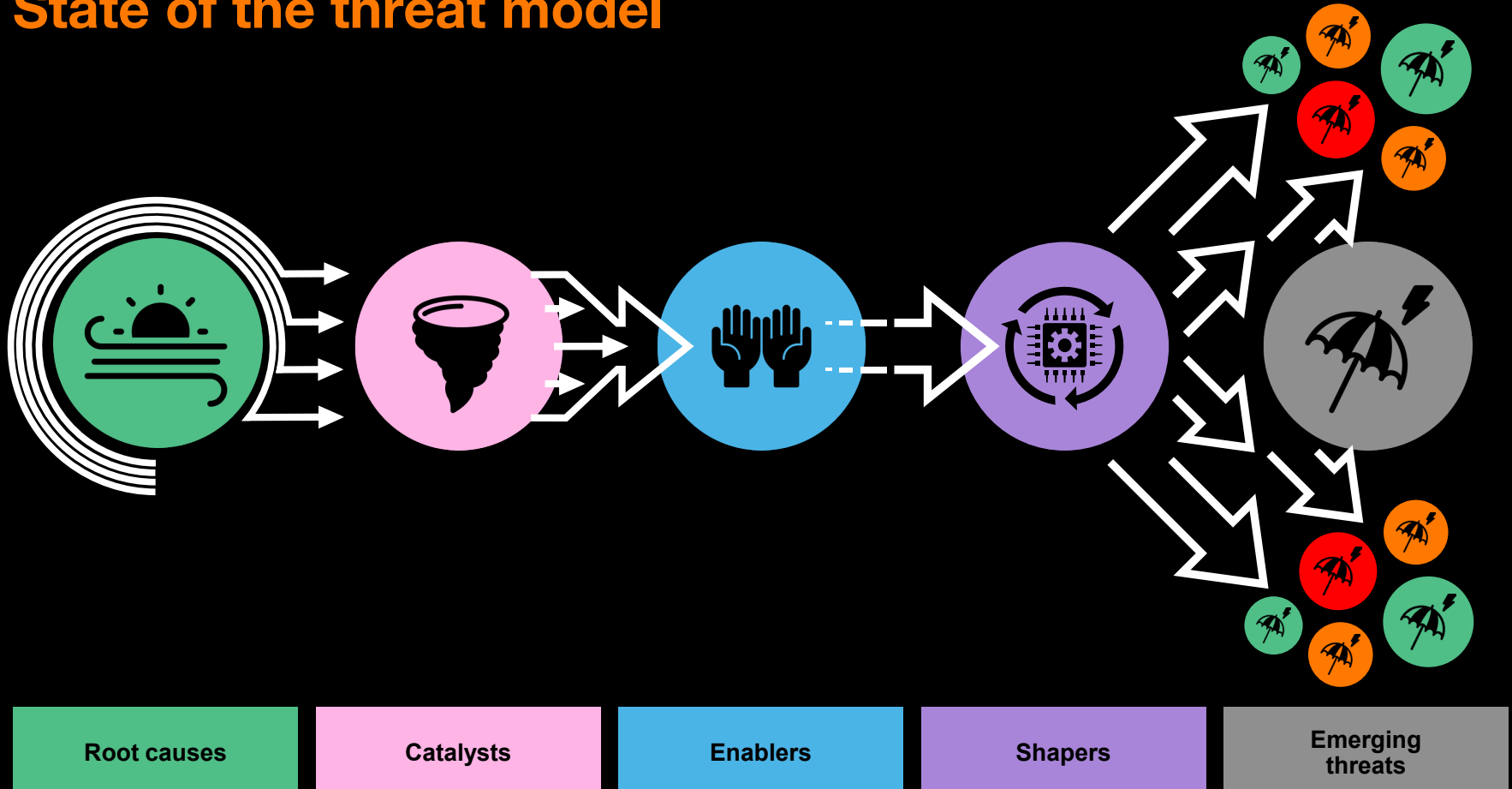
How World Watch intelligence is processed

■ Security Operations Center ■ CyberSOC Detection ■ CyberSOC Threat Hunting ■ Managed Vulnerability Scanning

- The intelligence-led approach in action: about half of the advisories are directly applicable in standard security operations
- Most signals could be directly put to use in Managed Vulnerability Scanning services
- 36% are reinforcing SOC/CyberSOC operations
- The other half can still be applied:
 - They are addressing specific issues with external providers (e.g. cloud services)
 - They require more strategic or tactical adjustments to avoid or mitigate



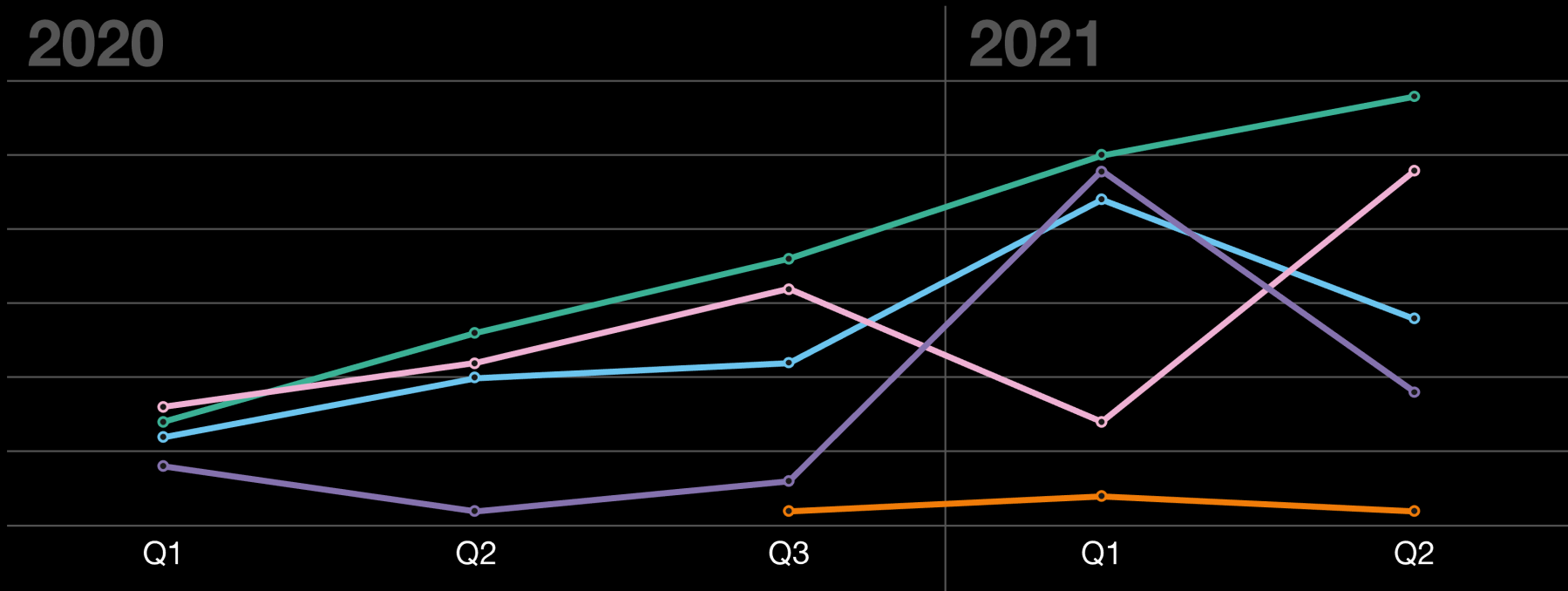
State of the threat model

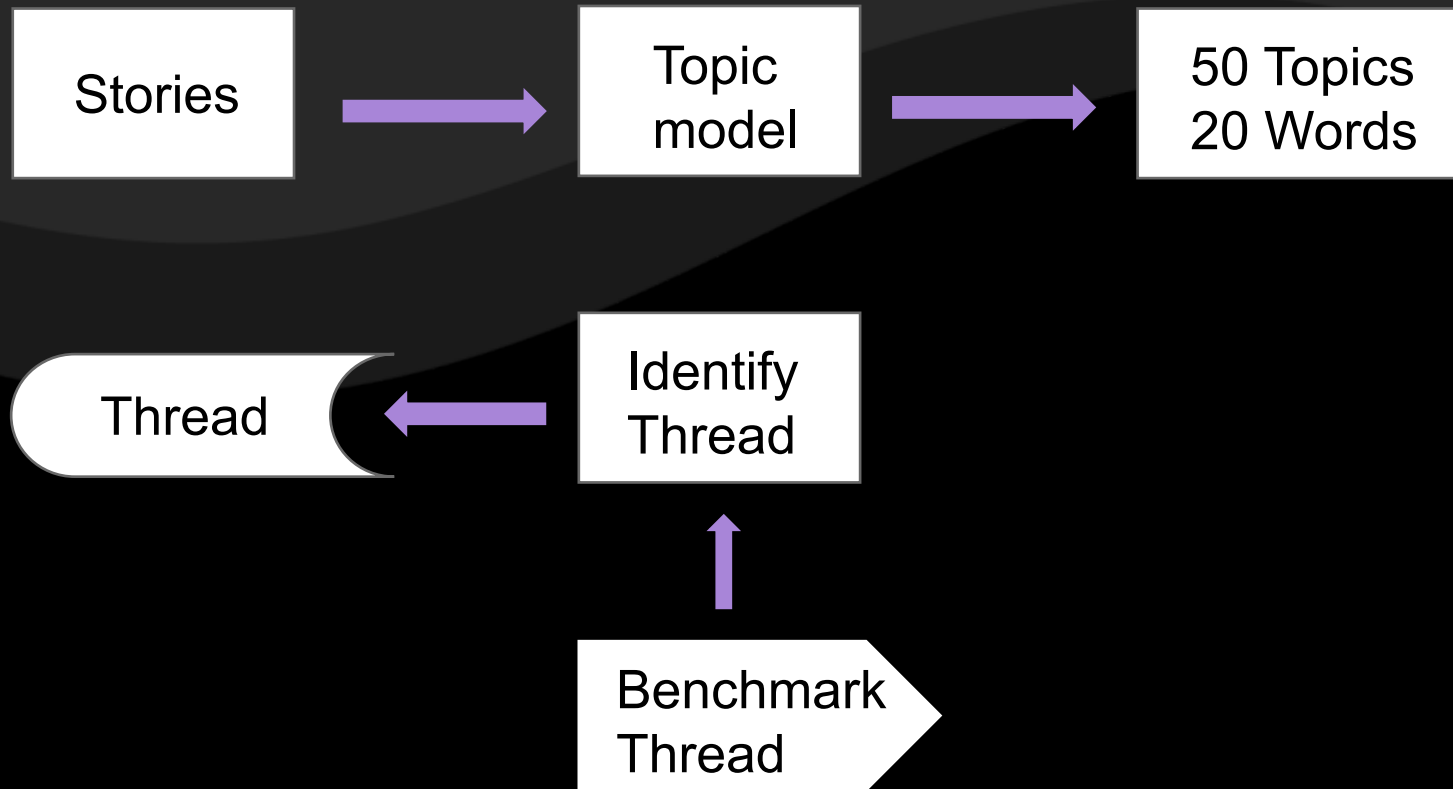


Systemic factors

and resultant threats in advisories

■ Attacks on Mobile Phones ■ Threats involving Security Products ■ Systemic Interdependence ■ Threats involving the Supply Chain ■ Threats involving Ransom





Orange
Cyberdefense



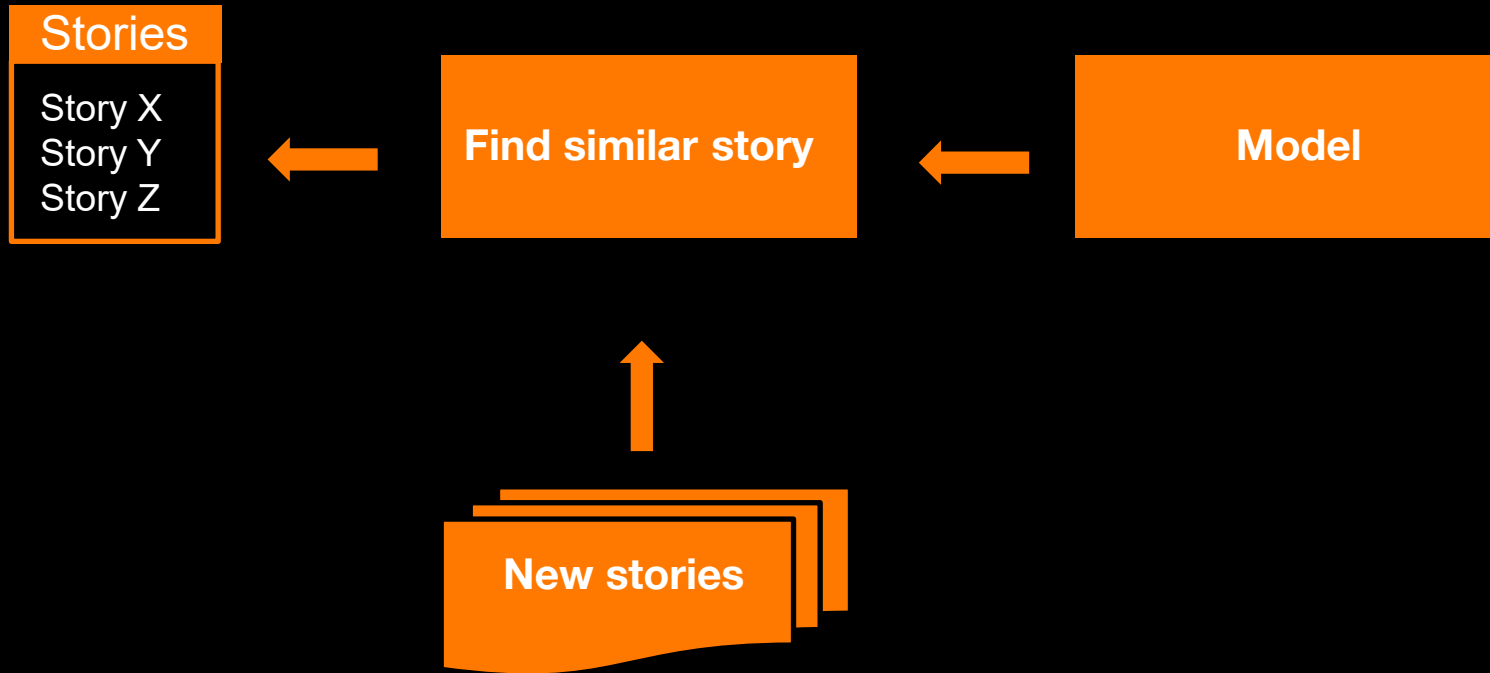
Stories



Topic
model



50 Topics
20 Words



NLP – Document Similarity: Predicts what other bodies of text closely resemble the reference document.

US sanctions NSO Group and three others for spyware and exploit sales		✕
Main category	News	
Categories	NEWS	
Urgency	Information	
Updated	01/12/2021	
Our reference	Signal: SIG-11598	
What you will hear	The U.S. has sanctioned four companies located in Israel, Russia, and Singapore for the development of spyware or the sale of hacking tools used by state-sponsored hacking groups.	

SIG-11598

MOTHERBOARD
TECH BY VICE

A Private Spy Was Caught Using a Hacking Tool to Target Their Crush

Brings back memories of the NSA agents who did the same thing.

By Ben Makuch

https://www.vice.com/en_us/article/n7i8dk/a-private-spy-was-caught-using-a-hacking-tool-on-their-crush

Congress wants to know what commercial spyware other countries are using

Intelligence funding bill for 2021 to mandate DNI to submit report to Congress about surveillance vendors and the countries that use spyware.

Written by **Catalin Cimpanu**, Contributor
Posted in Zero Day on June 11, 2020 | Topic: **Cybersecurity**

<https://www.zdnet.com/article/congress-wants-to-know-what-commercial-spyware-other-countries-are-using/>

SIGN IN The Register

United Nations calls for moratorium on sale of surveillance tech like NSO Group's Pegasus

Suggests the world to sort out a ban to preserve human rights, issues sternly worded 'Please Explain' to Israel

Simon Sharwood, APAC Editor

https://www.theregister.com/2021/08/13/un_wants_surveillance_tech_sales_moratorium/

SIG-11598 0.32316961884498596

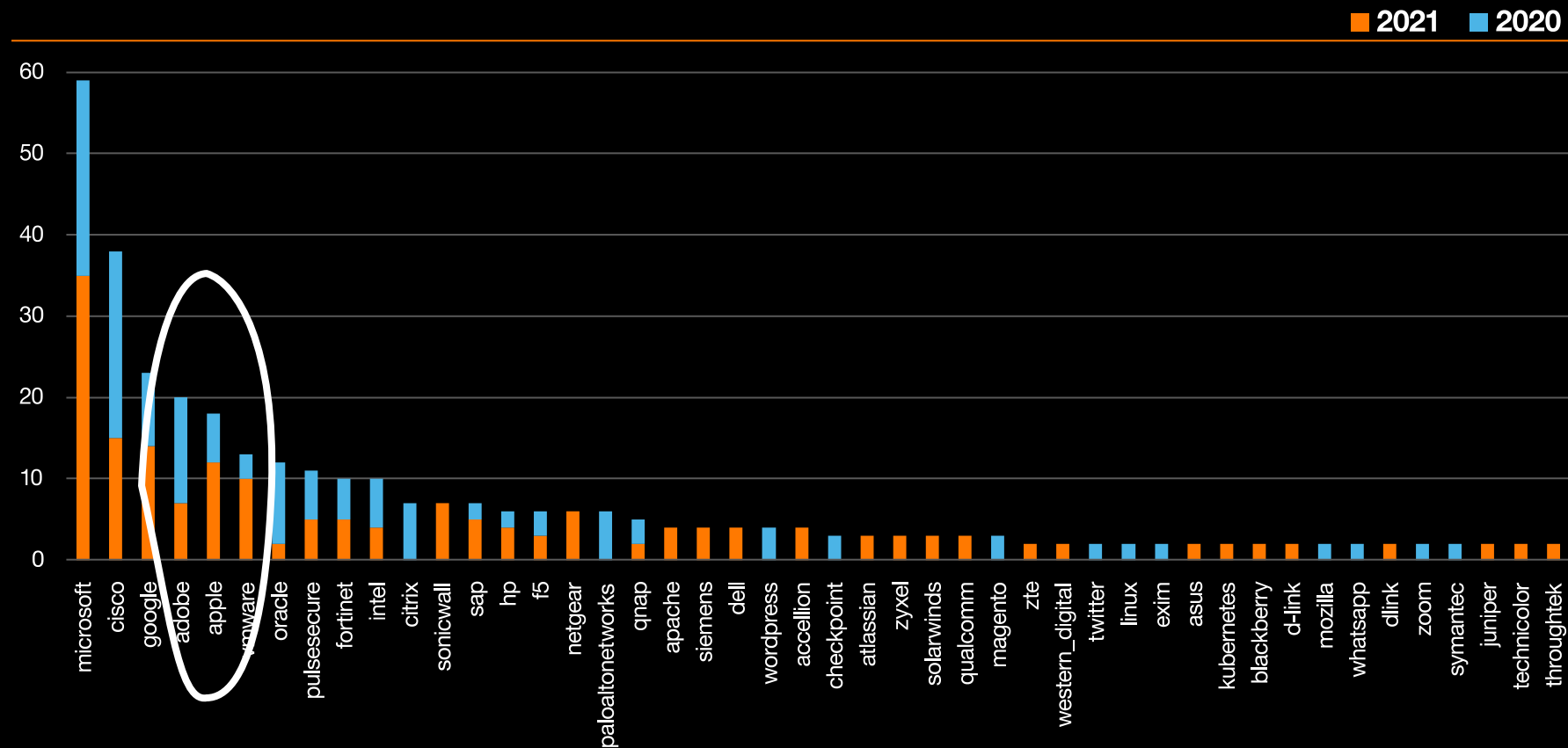
Orange
Cyberdefense

Implementing intelligence

Mobile security

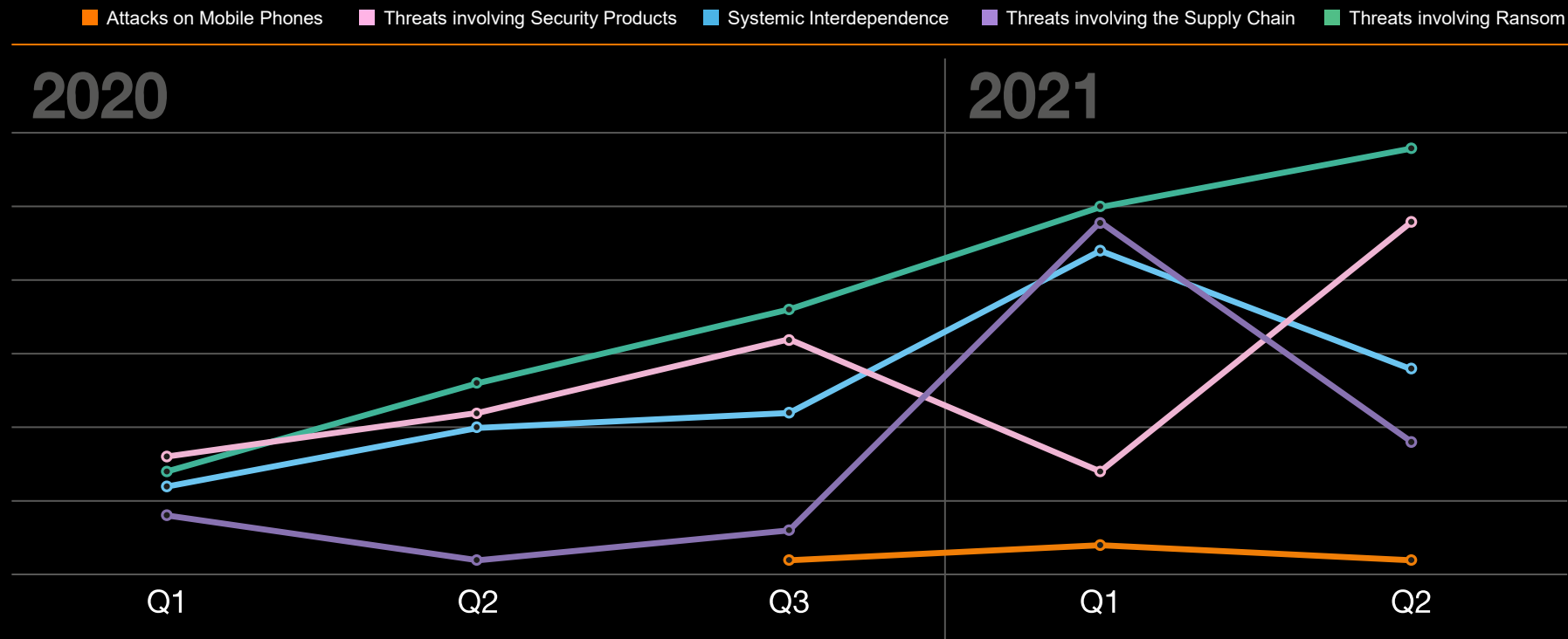
Technologies featuring in advisories

More than once in the past 12 months



Systemic factors

and resultant threats in advisories

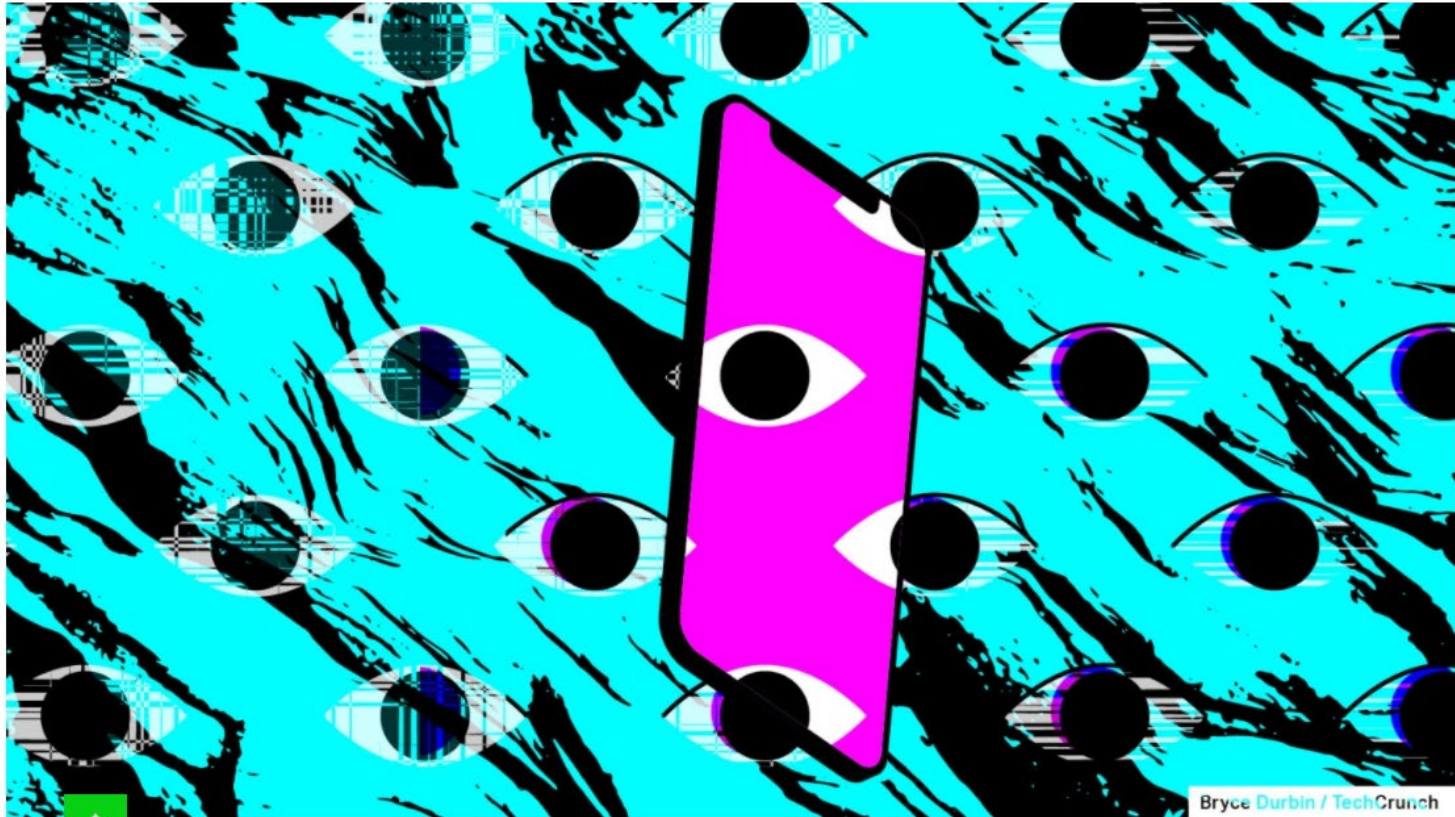


Apple patches an NSO zero-day flaw affecting all devices

Citizen Lab says the ForcedEntry exploit affects all iPhones, iPads, Macs and Watches

Zack Whittaker @zackwhittaker / 9:15 PM GMT+2 • September 13, 2021

 Comment



Bryce Durbin / TechCrunch

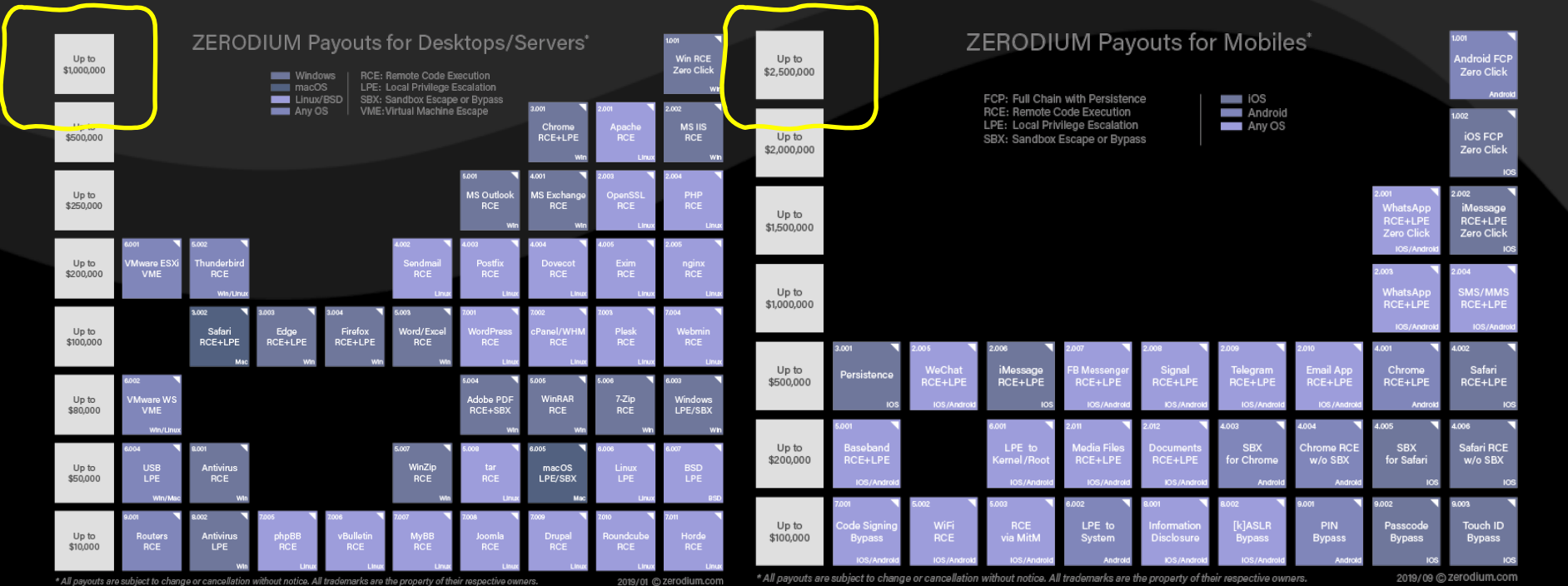


יחידה 8200



Governments can't possibly keep pace with demand, so a new breed of PMC emerges from the Military Industrial Complex, ready to offer its services.

Zerodium pays **BIG bounties** to security researchers to acquire their original and previously unreported zero-day research. While the majority of existing bug bounty programs accept almost any type of vulnerabilities and PoCs but pay very little, **at Zerodium we focus on high-risk vulnerabilities with fully functional exploits** and we pay the highest rewards in the market (**up to \$2,500,000 per submission**).







„I know
Your Secret, EVERY
while YOU
FUMBLE IN THE
Dark.“



News ▾ Middle East Documentaries ▾ Shows ▾ Investigations Opinion

Now: Philippines Manchester Bombing Nepal Indonesia Taiwan

NEWS | **HACKING** 13 MAY 2017



f Share

🐦 Tweet

💬 Comment

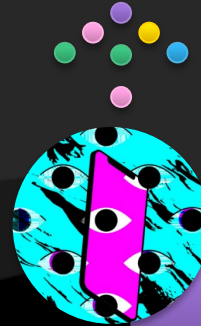
🖨️ Print

Europol: Ransomware attack is of unprecedented level

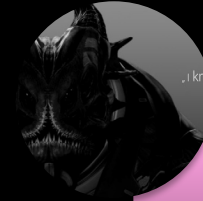
*International investigation needed to identify culprits of **biggest-of-its-kind** cyber-extortion attack, Europol says.*



An historical pattern to watch for



Unprecedented new threats, attacks & compromises



Government hacking investment leak into the civilian space



New types and levels of cybercrime are enabled by cryptocurrencies



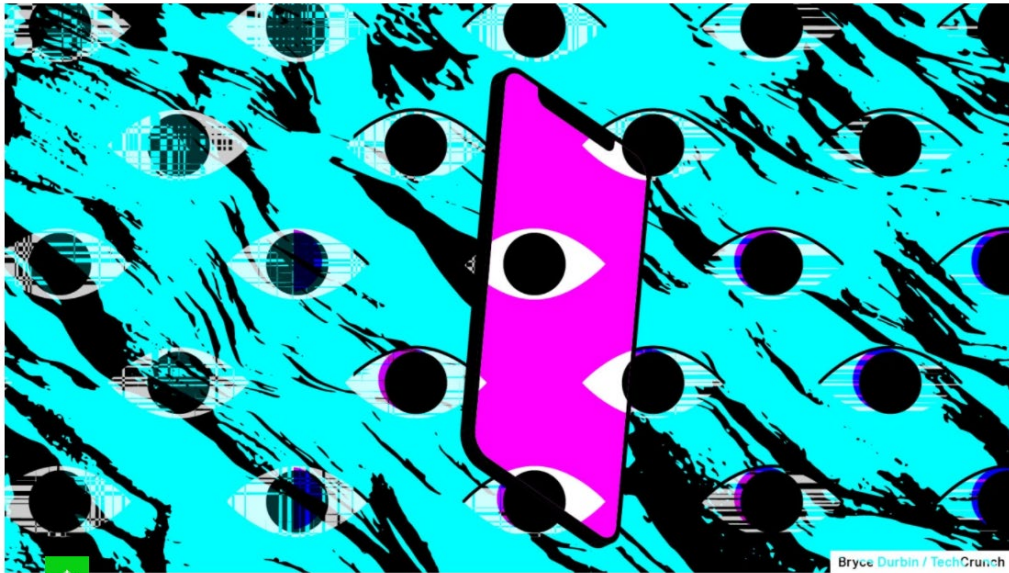
A cybercrime ecosystem hungry for new revenues

Apple patches an NSO zero-day flaw affecting all devices

Citizen Lab says the ForcedEntry exploit affects all iPhones, iPads, Macs and Watches




Zack Whittaker @zackwhittaker / 9:15 PM GMT+2 • September 13, 2021

[Comment](#)



Emerging threats

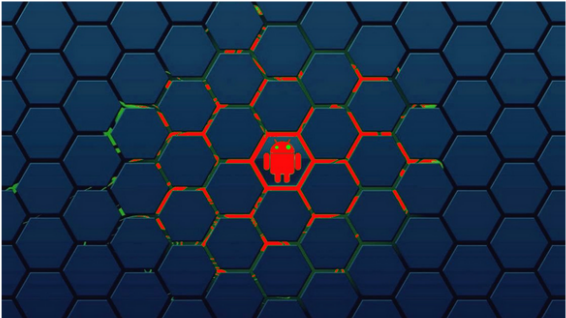
On mobile devices

BLEEPINGCOMPUTER   

NEWS • DOWNLOADS • VIRUS REMOVAL GUIDES • TUTORIALS • DEALS •

FluBot Android malware operation shutdown by law enforcement

By [Bill Toulas](#) June 1, 2022 09:31 AM 0



Europol has announced the takedown of the FluBot operation, one of the largest and fastest-growing Android malware operations in existence.

The malware operation's takedown resulted from a law enforcement operation involving eleven countries following a complex technical investigation to pinpoint FluBot's most critical infrastructure.

The participants in the operation were Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands, and the United States.





ZDNet Innovation Security Business Finance Education Home & Office More

Home / Innovation / Security

This new Android malware bypasses multi-factor authentication to steal your passwords

Cybersecurity researchers uncover MaliBot, a powerful new Android malware. Be careful what you download, and from where.

 Written by Danny Palmer, Senior Writer on June 16, 2022


   

A newly discovered form of Android malware steals passwords, bank details and cryptocurrency wallets from users – and it does so by bypassing multi-factor authentication protections.

The malware has been detailed by [cybersecurity researchers at F5 Labs](#), who've dubbed it MaliBot. It's the latest in a [string of powerful malware targeting Android users](#).

Ursnif Operators Leverage Cerberus to Automate Fraudulent Bank Transfers in Italy

Breaches and Incidents • June 29, 2021 • [Cyware Alerts - Hacker News](#)



Researchers have discovered a new variant of the Ursnif (aka Gozi) banking trojan that is actively targeting online banking users in Italy. The operators of this campaign are using Cerberus malware to sharpen the attack penetration.

What was discovered?

Ursnif is being delivered to Italian victims via malicious email attachments, typically posing as some business correspondence such as an invoice or some delivery notification.

- The infection chain usually comprises poisoned macros embedded inside productivity files commonly used in organizations. In some cases, attackers were observed specifically targeting Italian-based IP addresses.
- Once infected with the malware, users are tricked into downloading the [Cerberus Android malware](#) in the guise of a security app.
- Cerberus allows the attackers to receive two-factor authentication codes sent by the banks, which can be leveraged for further fraudulent activities.

World Watch

Free subscription



<https://www.orange cyberdefense.com/global/solutions/security-intelligence/world-watch>

Orange Cyberdefense

Build a safer digital society.