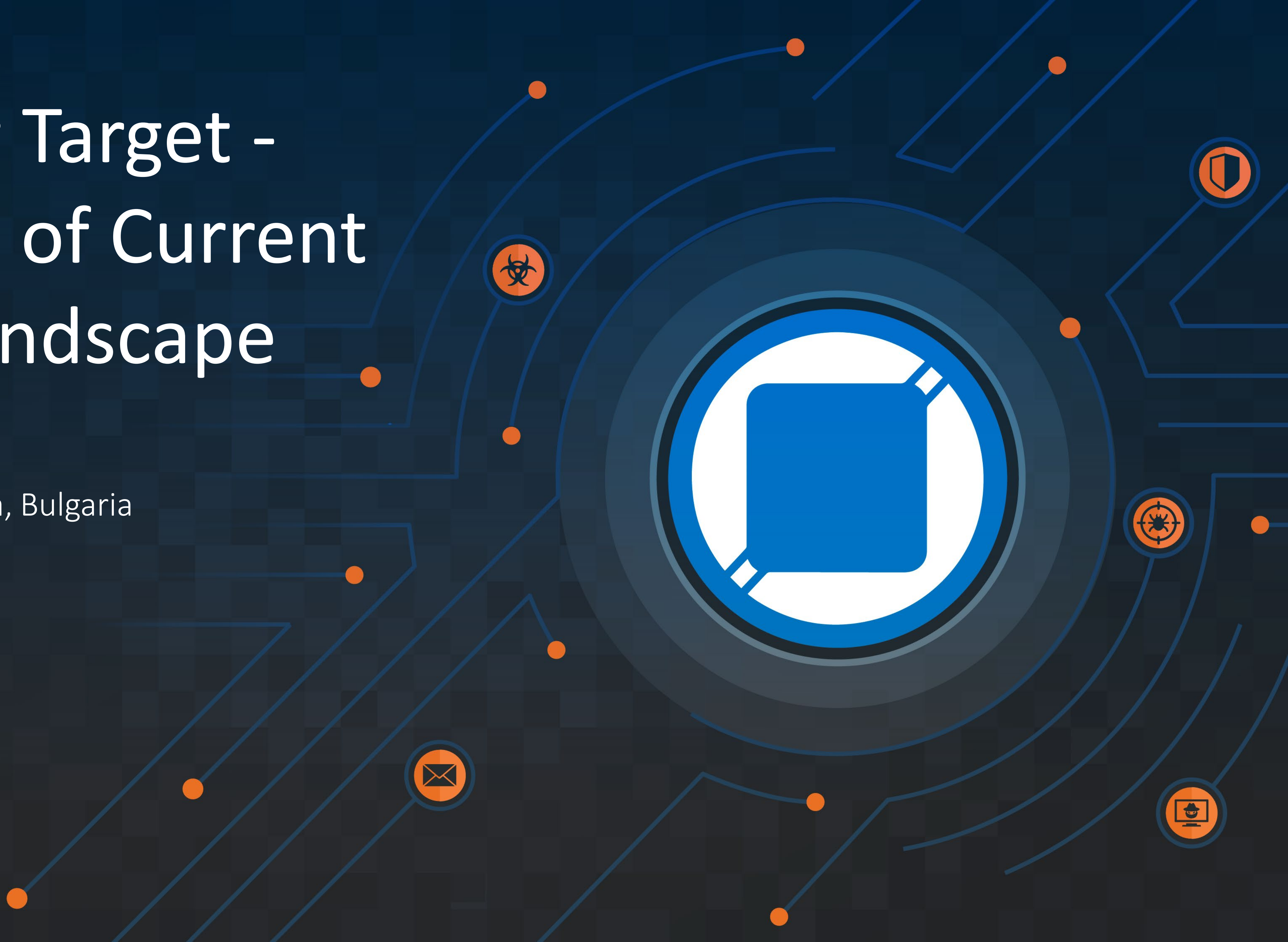
A Moving Target - Overview of Current Threat Landscape

BSides Sofia

23rd March 2024 , Sofia, Bulgaria



cisco Talos

Who am I?

Senior Incident Response Consultant

Supporting Cisco customers with emergency response and proactive activities, ranging from analysis of data of infected systems to creation of incident response documentation and simulation exercises.

Part of Cisco Switzerland

Gergana Karadzhova-Dangela

LinkedIn | B.Sc. in IT-Forensics, CISSP, GCFA

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

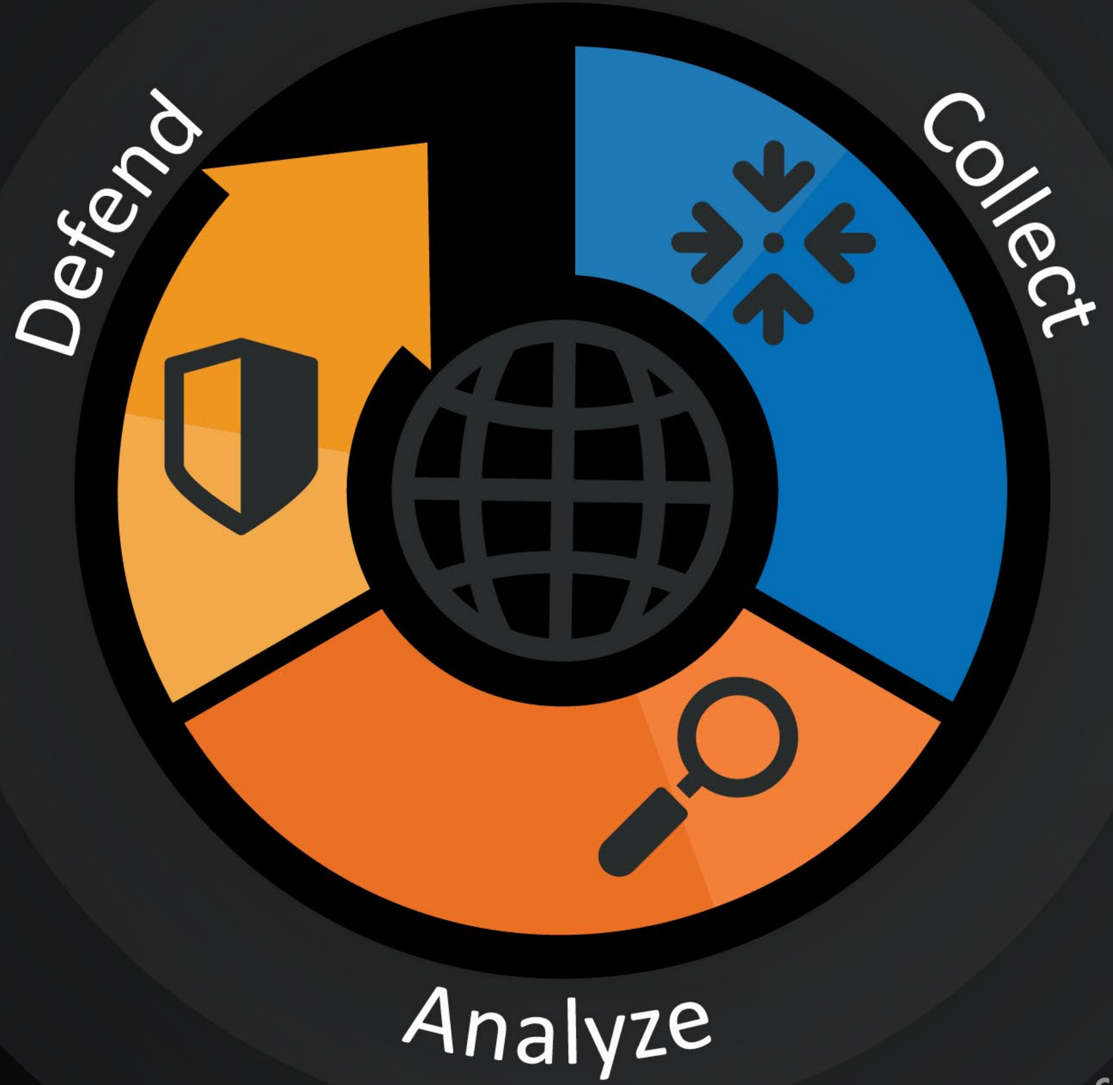
Agenda

1. Meet Cisco Talos
2. Threat landscape ⇔ Threat Intelligence
3. APT Groups
4. Ransomware
5. Top targeted vulnerabilities
6. Defense landscape

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Talos powers the Cisco portfolio with comprehensive intelligence

Every customer environment,
every event, every single day,
all around the world



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unmatched visibility across the threat landscape

550B security events/**day**

~9M emails blocked/**hour**

~2,000 new samples/**minute**

~2,000 domains blocked/**second**

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Intelligence Collection

Primary and secondary sources of threat intel

- Product telemetry
- Talos IR engagements
- Vulnerability research
- Intelligence partnerships
- Cutting-edge threat research
- Honeypots and spam traps

200+

Vulnerabilities discovered per year

60+

Government and law enforcement partnerships

45k

critical infrastructure endpoints monitored in Ukraine

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

(Cybersecurity) Threat Landscape

Dangers

Risks

Attacks

Potential

Ongoing

Threat actors

Vulnerabilities

Malware

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Goals may be different, but methodologies are similar

Different motivations

Cyber crime

- Financially motivated
- Phishing
- Big-game hunting
- Social engineering

State-sponsored

- Data and espionage
- Havoc and chaos
- Supply chain attacks
- Partner abuse

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Actors

Motivations across the spectrum

Cyber Criminal

Financially motivated

Access to
valuable data
Ransom -> Extortion

Nation State

Gain intelligence

Nuclear, Fin or Tech

Strategic Sabotage
Critical Infrastructure
Disruption

Ideologues

Spread message

Hackers, Terrorists
Anti-Capitalism
Anti-Corporate

Inspired by political and/or social issues

Thrill Seekers

Fame and glory

Experiments, learning
(don’t aim to cause damage)

Some become trolls - misinformation

Insiders

By Intent

Disgruntled employee
Unfair treatment
Different “goals”

By accident

© 2024 Cisco and/or its affiliates. A

Advanced Persistent Threats

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

APTs: China Summary

APTs operated at a rapid pace this year, conducting sophisticated and stealthy intrusions into numerous high-value targets.

Geopolitical gains

APTs occurred at a rigorous pace, likely in response to **geopolitical** events that strained the country's relationships with the West and Asia Pacific.

Preparing for future

Based on analysis of many malicious campaigns, **Beijing** may be directing more aggressive intelligence collection and prepositioning for future targeted attacks in these regions.

Ransomware persists

Talos observed several instances of ransomware actors compromising a target closely following a long-term, covert APT intrusion by using similar methods of initial access and deploying ransomware.

Telecommunications

We responded to several intrusions into telecommunications providers by China-affiliated APTs this year, particularly in areas that are of strategic interest to Beijing.

Regional tensions

Rising tensions between China and Taiwan, China has also become increasingly aggressive in the South China Sea and relationship with Japan has also seen challenges in the past year.

Evasion techniques

Threat actors are deeply entrenching themselves in targeted networks and dodging detection.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat actor highlight: Volt Typhoon

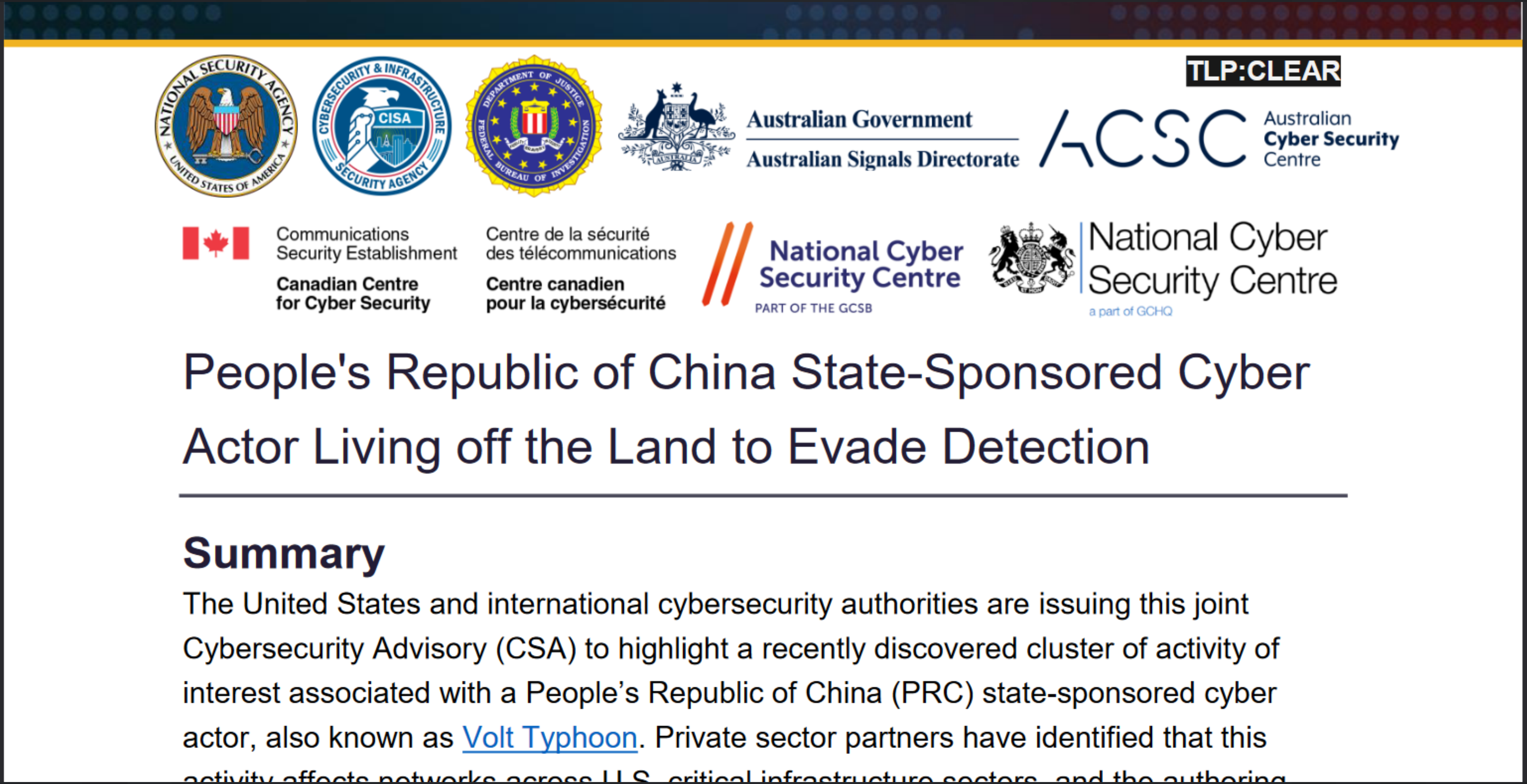
A China-affiliated threat group that made headlines this past year for their long-term operation targeting U.S. critical infrastructure organizations and military bases.

Talos investigated a sustained Volt Typhoon intrusion targeting the telecommunications sector in Guam, which is notably the site of a U.S. military base significant for the defense of Taiwan.

Our research revealed the actors maintained persistent access to and exfiltrated data from networks of a service provider and certain high-value customers for at least a year and a half.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Volt Typhoon (January 2024)



TLP:CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

The United States and international cybersecurity authorities are issuing this joint Cybersecurity Advisory (CSA) to highlight a recently discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon. Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring

Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

cisco © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

APTs: Russia Summary

Threats from Russian state-sponsored or state-aligned advanced persistent threats (APTs) remain a mainstay in our threat tracking and research efforts this year.

Gamaredon

Broadly suspected to be a team of Russian government-supported actors based in Crimea, the group in recent months has concentrated their efforts on cyberespionage against Ukrainian entities.

Turla

Conducts long-term espionage and data exfiltration operations that are in line with Russian intelligence priorities that the U.S. government attributes to a unit within the FSB.

Turla's Snake

For nearly 20 years, APT Turla deployed Snake to steal and exfiltrate data from targeted systems through numerous relay nodes scattered around the world.

Internal Task Unit

We've continued monitoring suspicious activity in endpoint telemetry for nearly three dozen Ukrainian partners across critical infrastructure sectors, including government, utilities, financial services, health care, and transportation.

Russia-Ukraine war

The task unit has continuously responded to a myriad of cyber threats since the onset of the Russia-Ukraine war, the observed activity in 2023 was far less sophisticated than what is typically associated with the sophisticated adversaries.

SmokeLoader Malware

We observed a spike in SmokeLoader activity in late April and early May, aligning with CERT-UA's reporting of mass distribution of SmokeLoader targeting Ukrainian entities.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

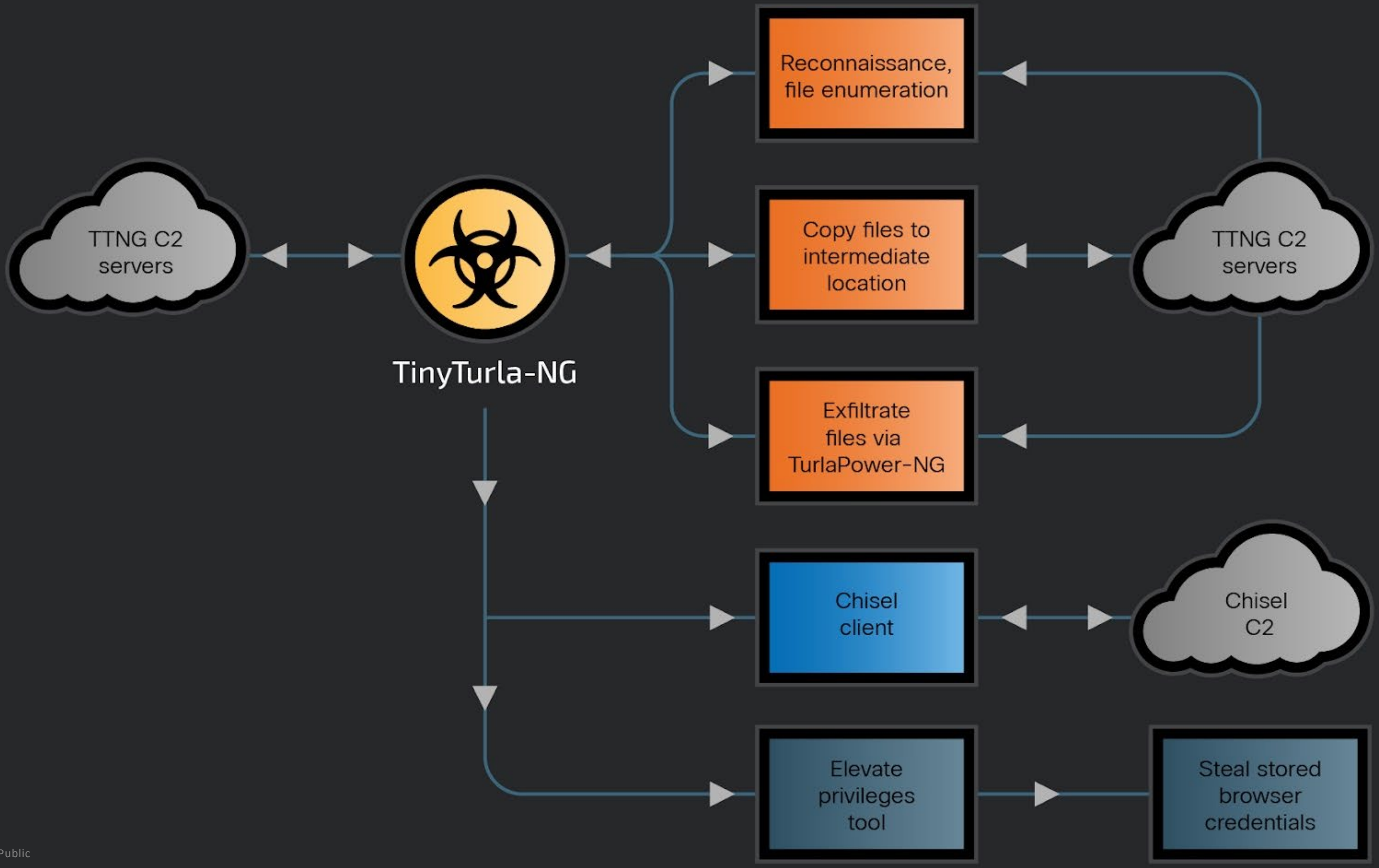
Turla

Turla instrumenting TTNG for various tasks

Russian espionage group Turla deploys new implant TinyTurla-NG (TTNG)

Deep dive: TTNG tooling and C2 analysis (Feb 2024)

Deep dive: TTNG post-compromise activity (March 2024)


TTNG C2 servers
TinyTurla-NG
Reconnaissance, file enumeration
Copy files to intermediate location
Exfiltrate files via TurlaPower-NG
TTNG C2 servers
Chisel client
Chisel C2
Elevate privileges tool
Steal stored browser credentials

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

2023

CISCO TALOS

YEAR IN REVIEW

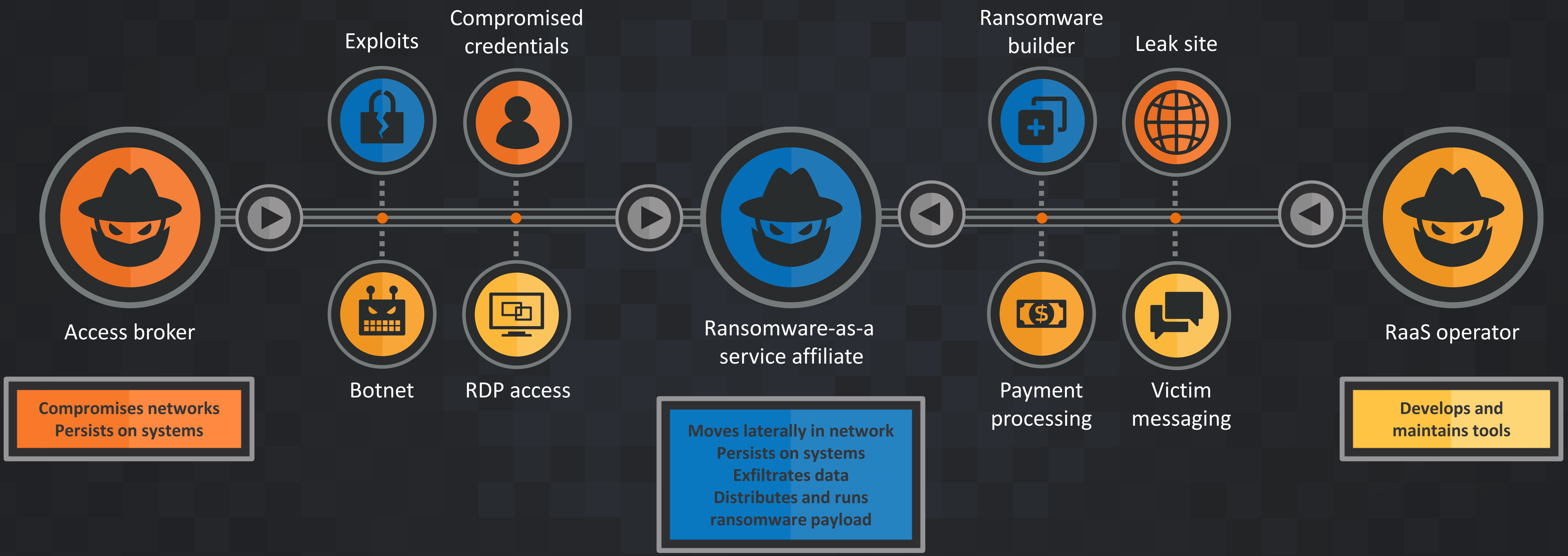
Read the full report on the Talos Blog
https://blog.talosintelligence.com/2023-year-in-review/

CISCO © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ransomware and Extortion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ransomware-as-a-service (RaaS)



Source: https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#ransomware-as-a-sevice-incidents

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ransomware and extortion summary

2023 Talos Year in Review

Ransomware global prevalence continues as new affiliate groups and techniques emerge. Groups increasingly shifting toward pure **data theft extortion** as defender community detection increases.

20%

Of incidents seen by Talos IR in 2023 involved ransomware

33%

Of incidents seen by Talos IR in Q2 2023* were data extortion.

25%

LockBit accounted for 1/4 of victim posts on data leak sites

1. LockBit again most prolific RaaS gang
2. Healthcare most targeted vertical Talos IR observed
3. Leaked source code enables less skilled actors into space
4. Exploitation of zero-day vulns rampant as Clop expertise broadens

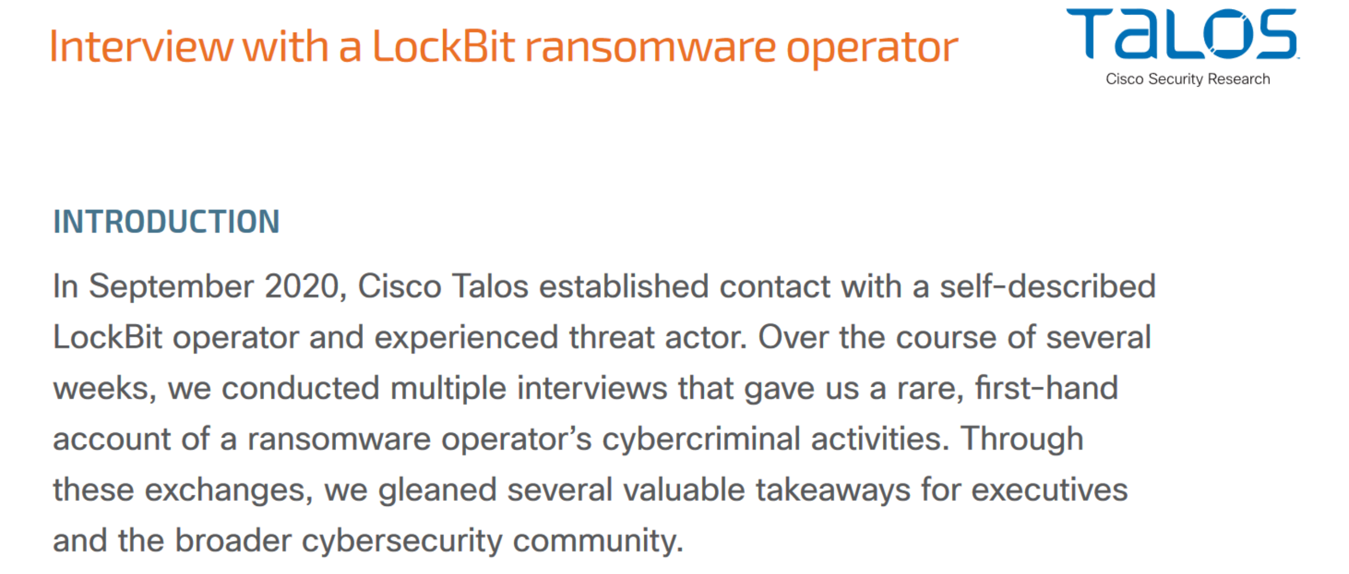
*25% increase over prior quarter

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

LockBit takedown - February 2024

LockBit Background:

Interview with a LockBit Ransomware Operator (2021)



Interview with a LockBit ransomware operator

TALOS
Cisco Security Research

INTRODUCTION

In September 2020, Cisco Talos established contact with a self-described LockBit operator and experienced threat actor. Over the course of several weeks, we conducted multiple interviews that gave us a rare, first-hand account of a ransomware operator's cybercriminal activities. Through these exchanges, we gleaned several valuable takeaways for executives and the broader cybersecurity community.

LockBit takedown:

- 20th Feb 2024 – The US Department of Justice joined the United Kingdom and international law enforcement partners in London today to announce the disruption of the LockBit ransomware group…
- 22nd February 2024 – LockBit relaunches its services

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

LockBit comeback – March 2024

Why the LockBit takedown is emblematic of the problems law enforcement face when stopping ransomware groups

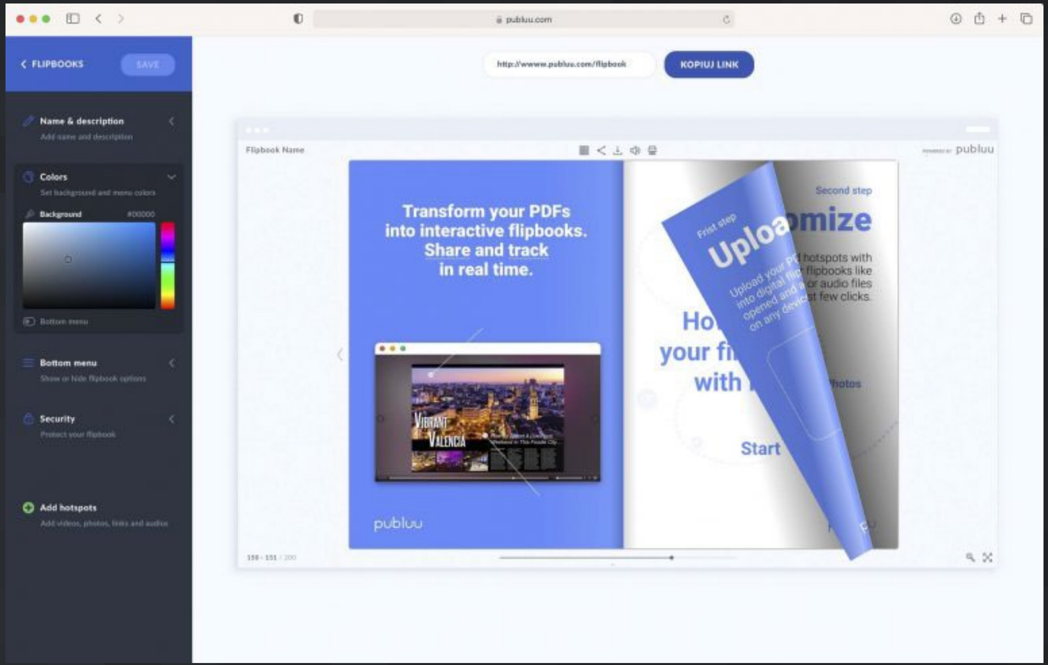
Read the full Talos blog here: https://blog.talosintelligence.com/p/48f2b2fd-723d-4fba-a634-bce5e764584a/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Phishing via digital document publishing sites

A new way to lure users into sharing their credentials

What is a digital document publishing site?



Transform your PDFs into interactive flipbooks. Share and track in real time.

Talos IR observed legitimate digital document publishing (DDP) sites being used for phishing, credential theft and session token theft.

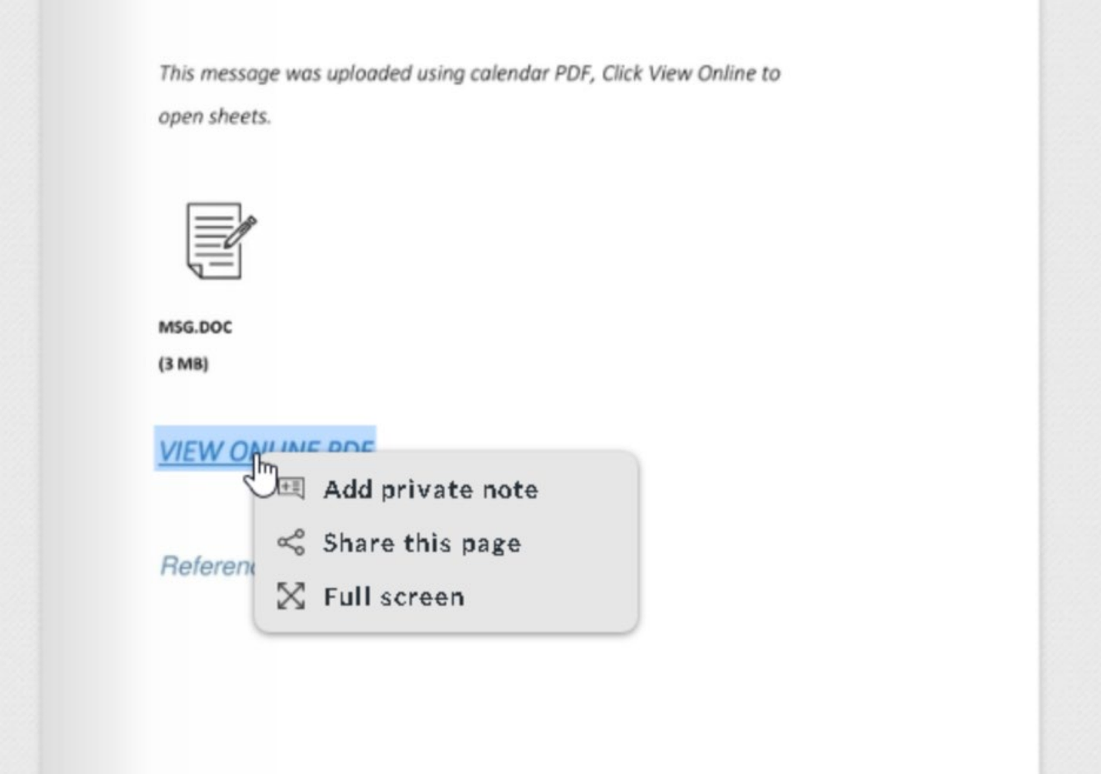
Image source: https://publuu.com/knowledge-base/how-to-make-an-ebook-with-publuu/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Malicious link detection in DDP

DDP productivity features may inhibit malicious link detection.

Read the full Talos blog here: https://blog.talosintelligence.com/threat-actors-leveraging-document-publishing-sites/ (March 2024)



This message was uploaded using calendar PDF, Click View Online to open sheets.

MSG.DOC

(3 MB)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Impact of leaked ransomware source code

Multiple leaks of ransomware source code and builders have had a significant effect on the ransomware threat landscape.

Rise of novice actors

Multiple leaks of ransomware source code and builders — components essential to creating and modifying ransomware — allowed ransomware operators to rebrand or give unsophisticated actors the ability to generate their own ransomware more easily with little effort or knowledge.

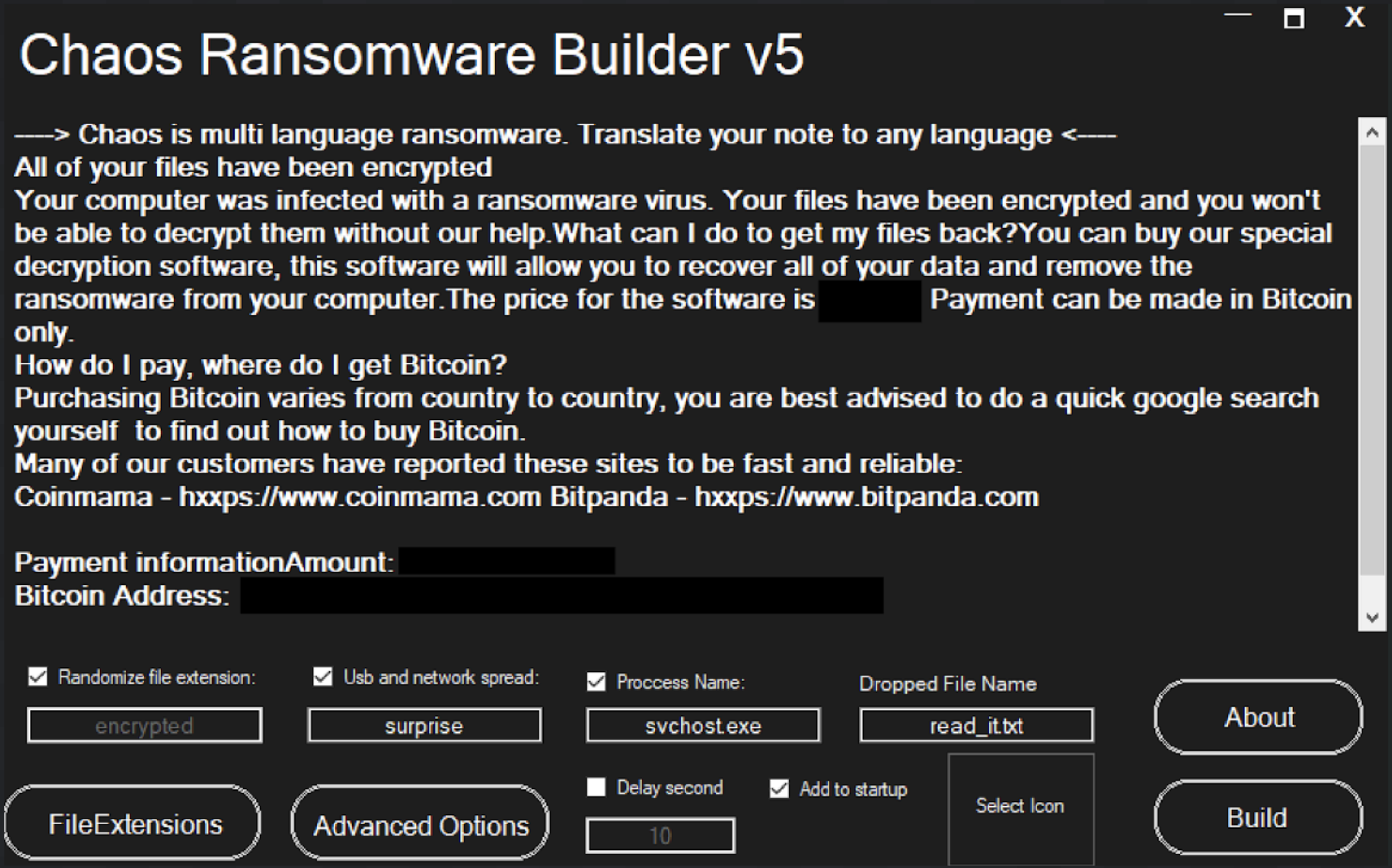
New ransomware strains

Talos observed a surge in new ransomware strains emerging from the Yashma ransomware builder.

In April, we discovered a new ransomware actor, RA Group, deploying their ransomware variant based on the leaked Babuk source code.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Chaos ransomware builder



----> Chaos is multi language ransomware. Translate your note to any language <----
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't be able to decrypt them without our help.What can I do to get my files back?You can buy our special decryption software, this software will allow you to recover all of your data and remove the ransomware from your computer.The price for the software is [redacted] Payment can be made in Bitcoin only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search yourself to find out how to buy Bitcoin.
Many of our customers have reported these sites to be fast and reliable:
Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com

Payment informationAmount: [redacted]
Bitcoin Address: [redacted]

☑ Randomize file extension: encrypted

☑ Usb and network spread: surprise

☑ Proccess Name: svchost.exe

Dropped File Name: read_it.txt

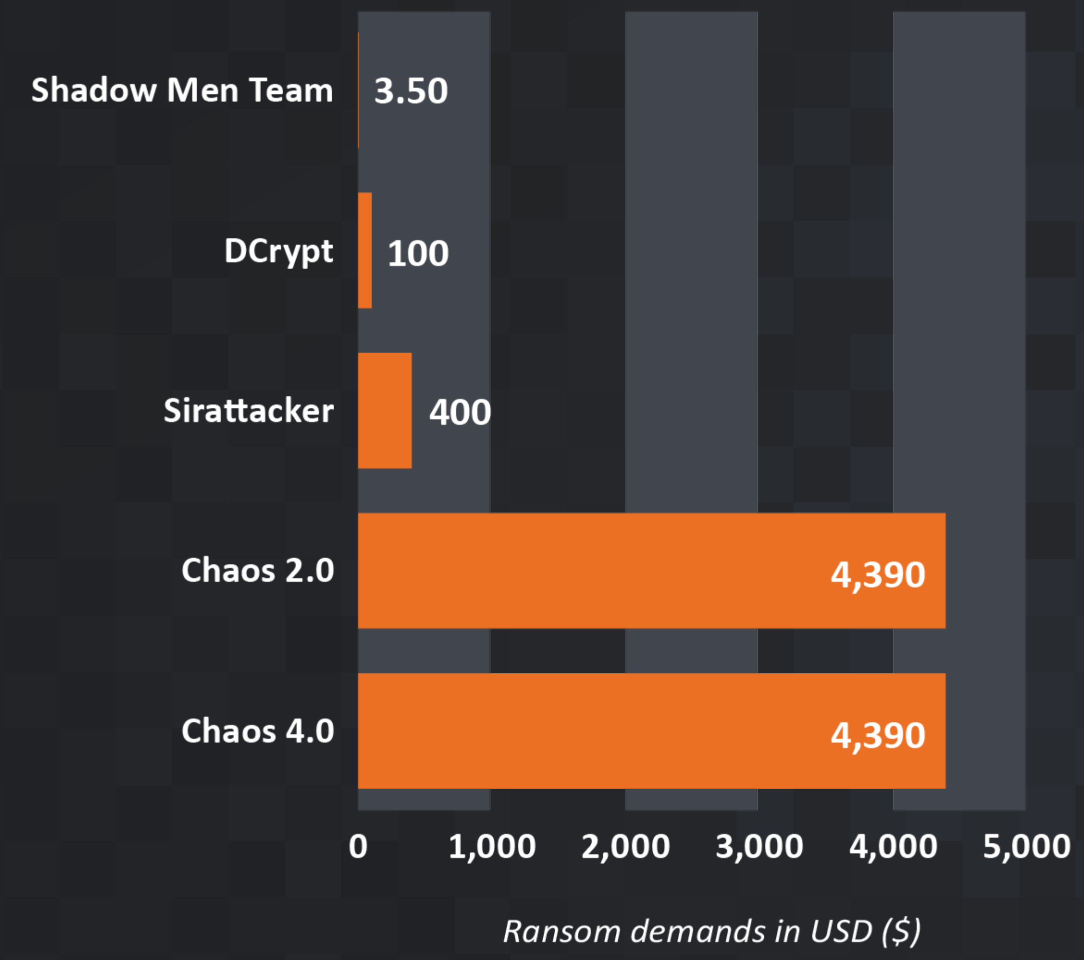
☐ Delay second: 10

☑ Add to startup

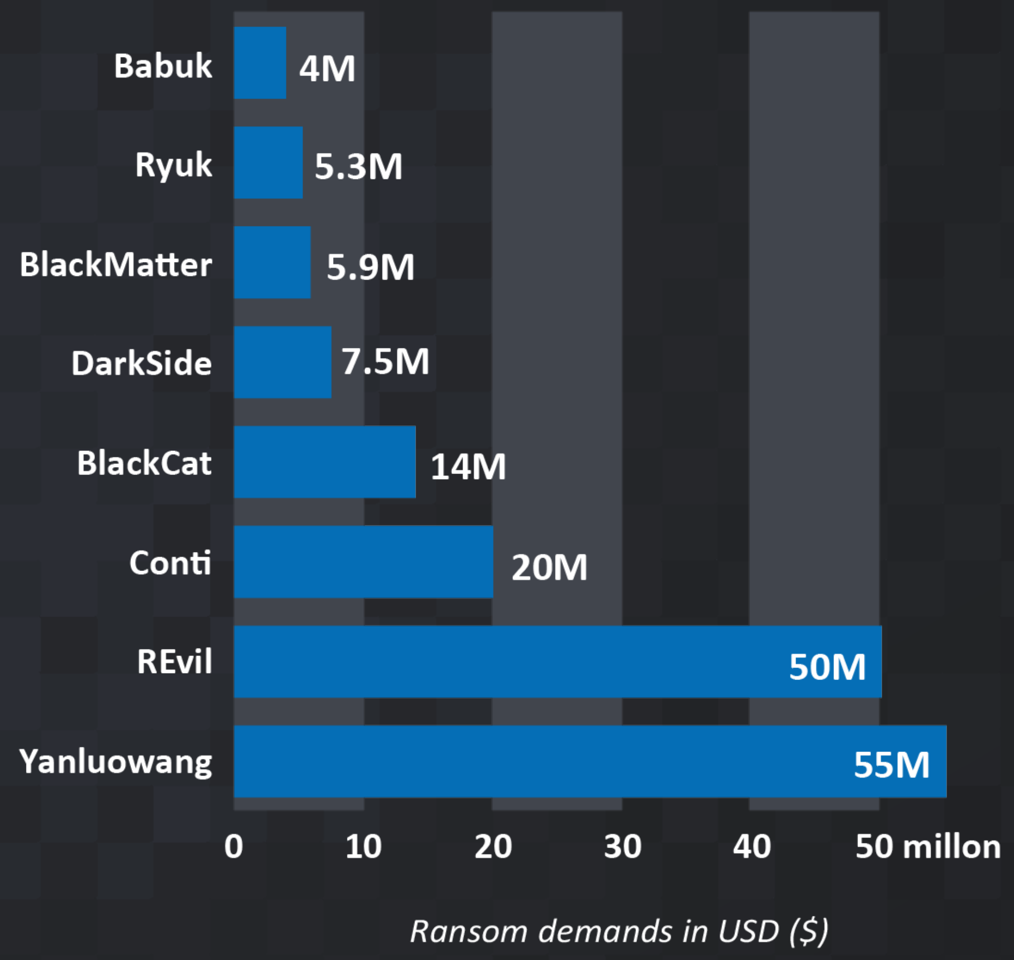
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ransom demands - comparison of leaked code-based variants vs. prominent groups

Leaked code-based ransomware variants



Prominent ransomware groups



Read the full Talos blog here: https://blog.talosintelligence.com/code-leaks-new-ransomware-actors/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Top targeted vulnerabilities

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Top targeted vulnerabilities

Ranking	CVE	Vendor	Product	CISA findings	CISA KEV catalog	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office and WordPad	Routinely exploited in 2022	Yes	100/9.3
2	CVE-2017-11882	Microsoft	Exchange server	Routinely exploited in 2022	Yes	100/9.3
3	CVE-2020-1472	Microsoft	Netlogon	Routinely exploited in 2022	Yes	100/9.3
4	CVE-2012-1461	Gzip file parser utility	Multiple antivirus products			58/4.3
5	CVE-2012-0158	Microsoft	Office	Commonly exploited by state-sponsored actors from China, Iran, North Korea, and Russia (2016-2019)	Yes	100/9.3

Source: *Cisco Secure Endpoint*

CISA sources: *Top Routinely Exploited Vulnerabilities, 2022 and 2016 - 2019.*

- Exploitation of older software vulnerabilities in commonly used applications
- Low cost/high impact target for threat actors

Key takeaway

Prioritize security patching of all systems in your enterprise

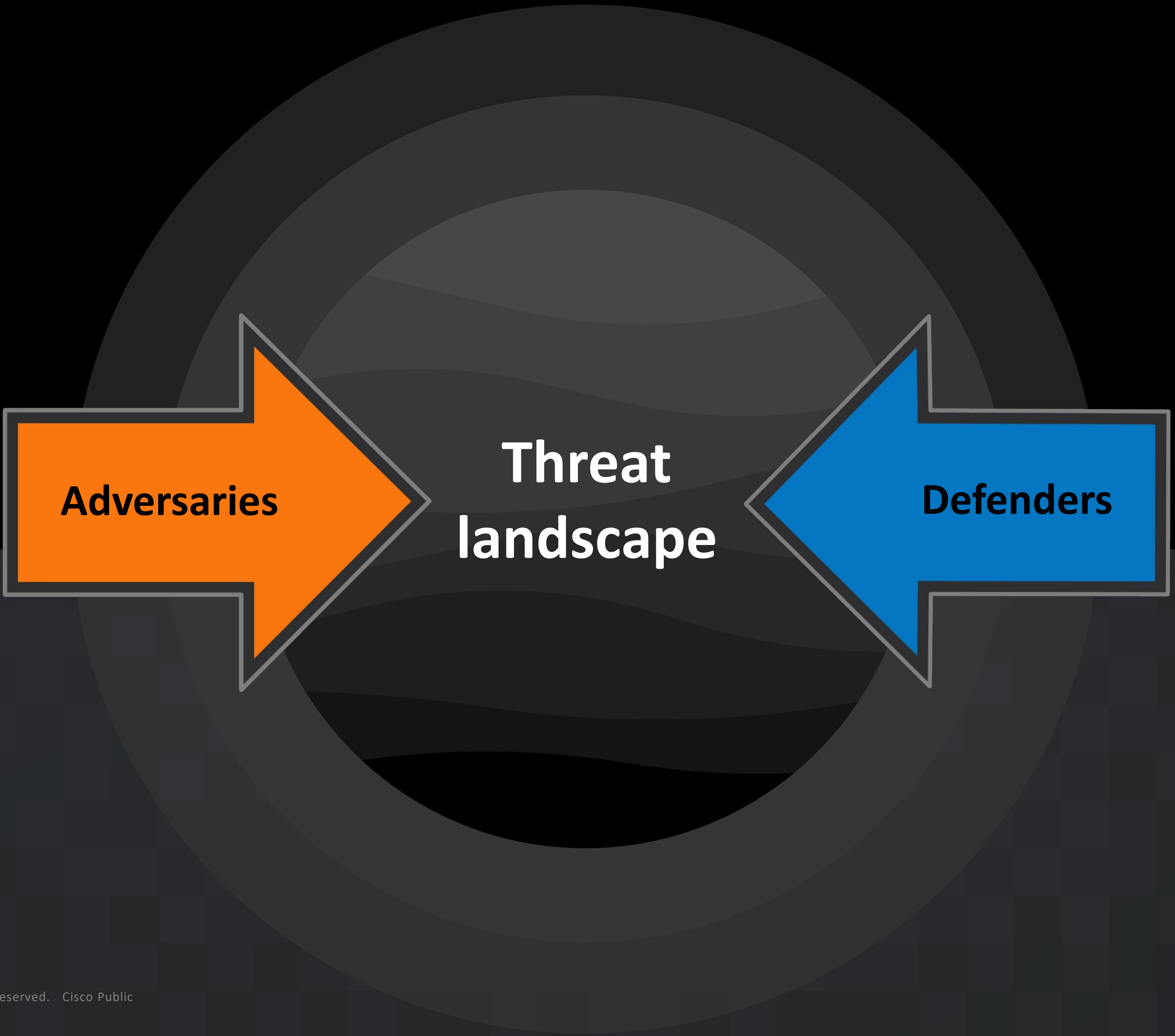
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Defense Landscape

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Sophistication and Persistence

Adversaries are more determined and persistant than ever



Adversaries

Threat landscape

Defenders

Inventiveness and Collaboration

The defender community's diligence, inventiveness and collaborative efforts are helping to push adversaries back

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolving defender landscape

AI Support

Configuration of security tools

Threat Intel Alliances

Private and public threat intel exchange

Information Sharing and Analysis Center (ISAC)

Regulations

Higher cybersecurity requirements for non-critical infrastructure organizations

NIS2
SEC

Increased awareness

Digitalization of public services

Recommended Talos community resources

Sign up - Weekly Talos Threat Source newsletter

Read - Quarterly Threat Overview reports

Tune in - Talos Takes Podcast episodes

Sign up here

Once per quarter, the key facts

Listen to our episode on malicious Windows drivers

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stay Connected and Up To Date

White papers, articles & other information
talosintelligence.com

ThreatSource Newsletter
cs.co/TalosUpdate

Talos Blog
blog.talosintelligence.com

Social Media Posts
Twitter: @talossecurity

Instructional Videos
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public