Kuwait 5th ERM Conference

Threat Landscape Overview

Secureworks®

January 2019

Rafe Pilling

Senior Security Researcher

Counter Threat Unit

SecureWorks in Numbers

70

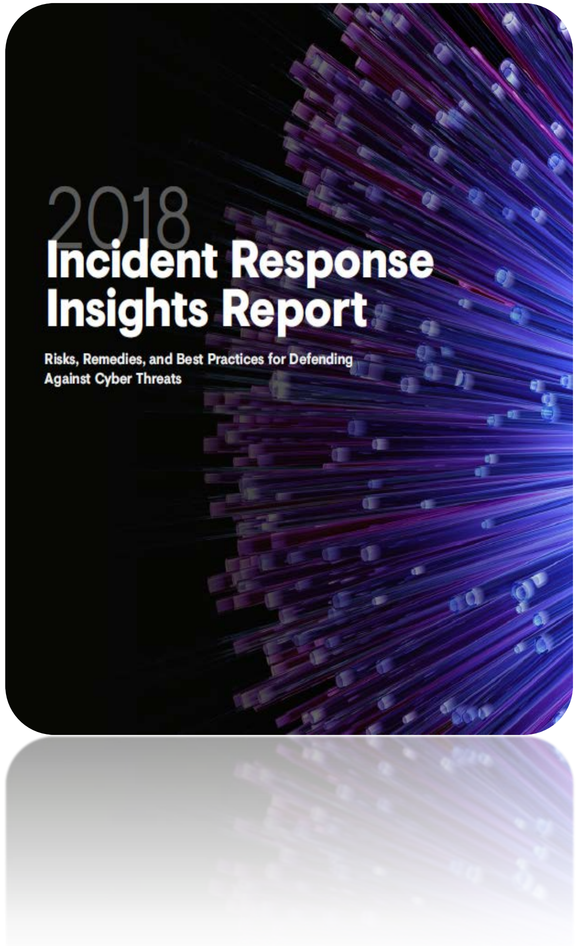
4 300

260 000 000 000

95 000 000 000 000

Overview of two 2018 reports

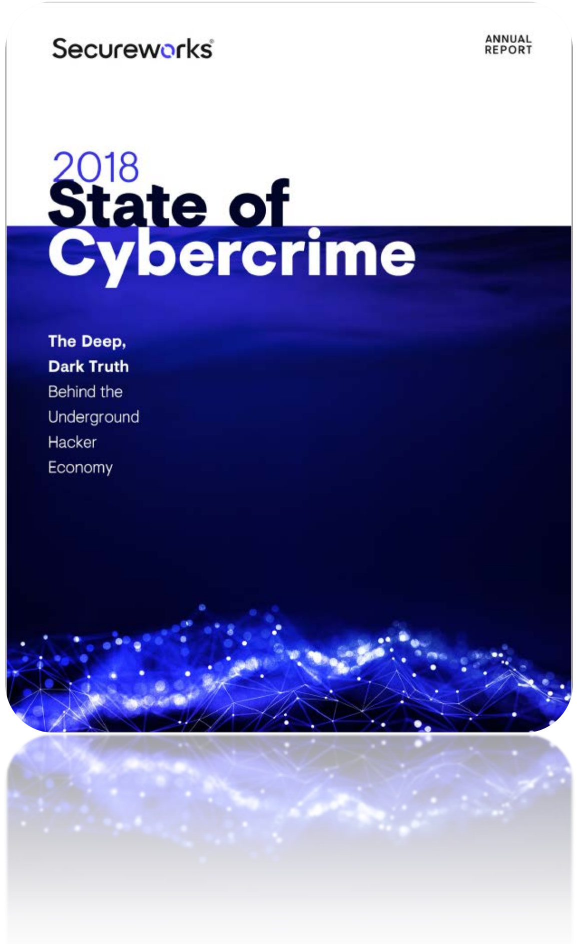
Reports available on line at www.secureworks.com



2018

Incident Response Insights Report

Risks, Remedies, and Best Practices for Defending Against Cyber Threats



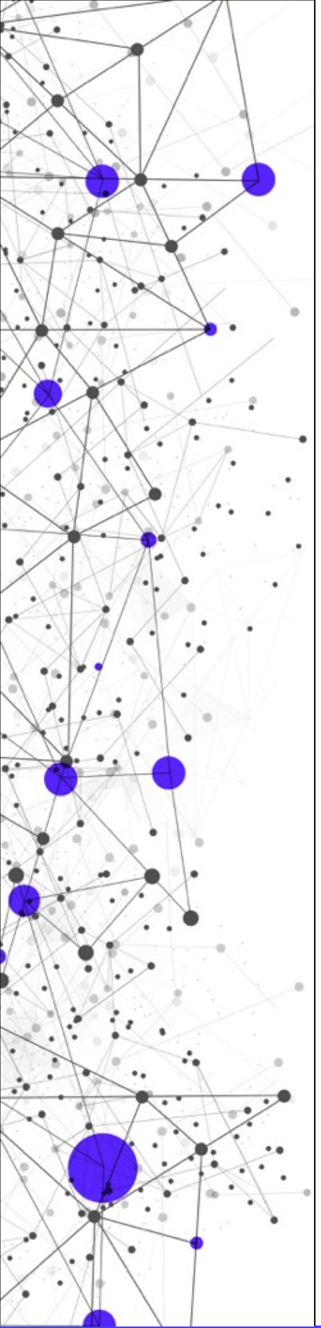
Secureworks

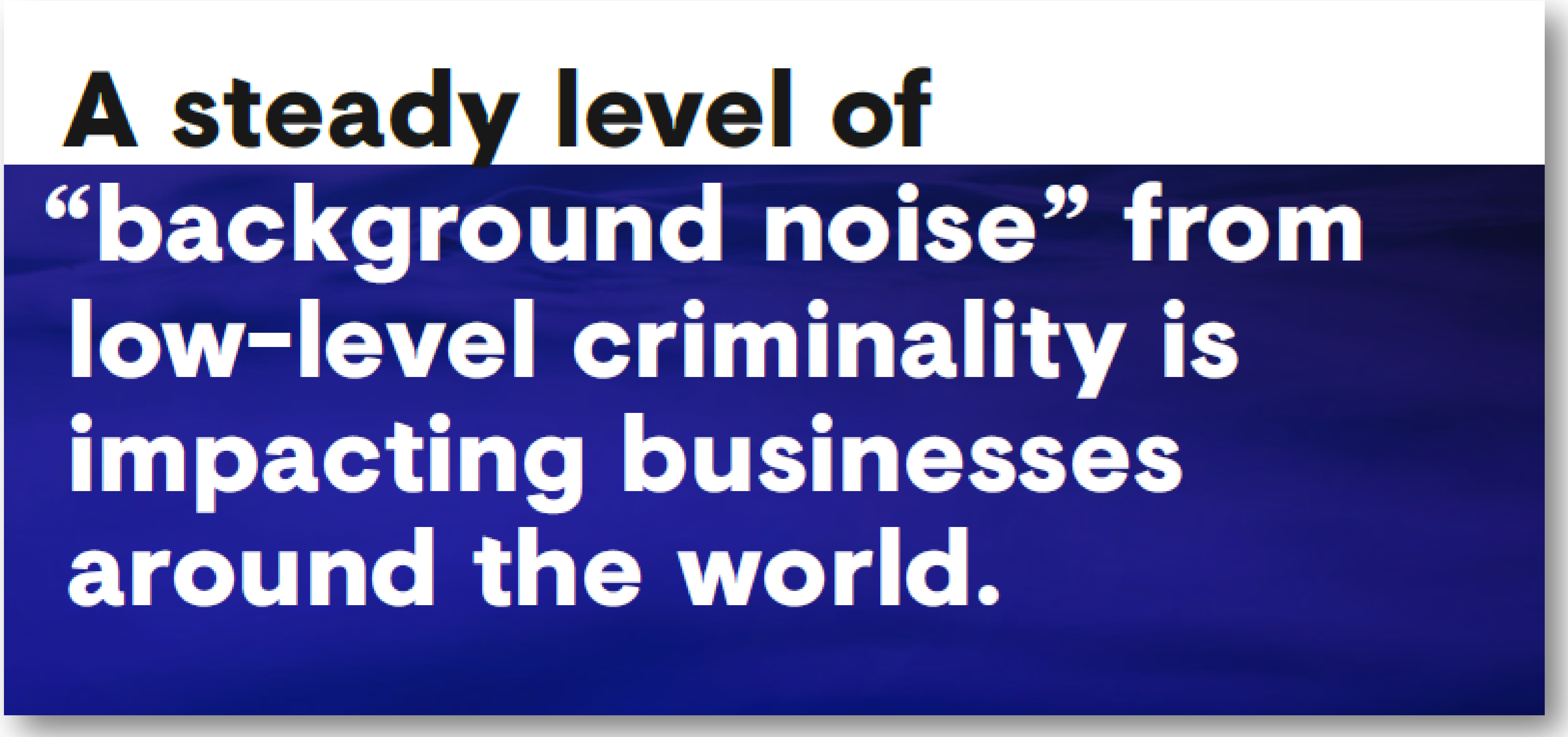
ANNUAL REPORT

2018

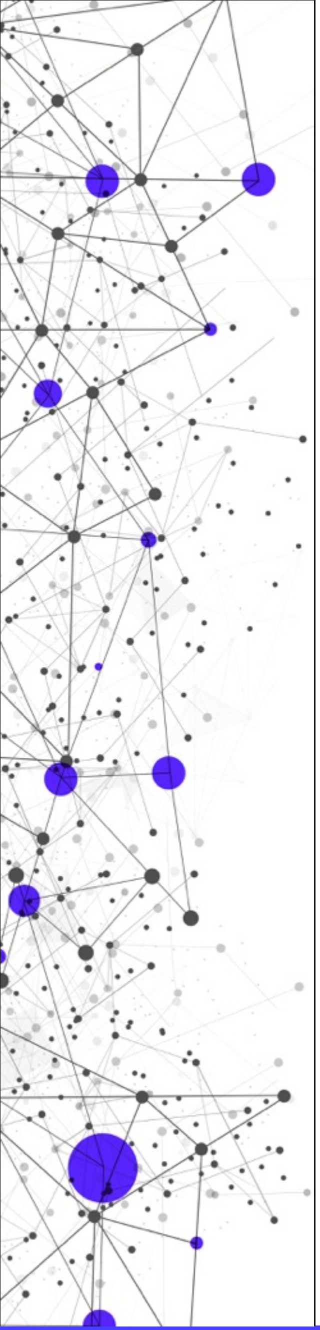
State of Cybercrime

The Deep, Dark Truth Behind the Underground Hacker Economy





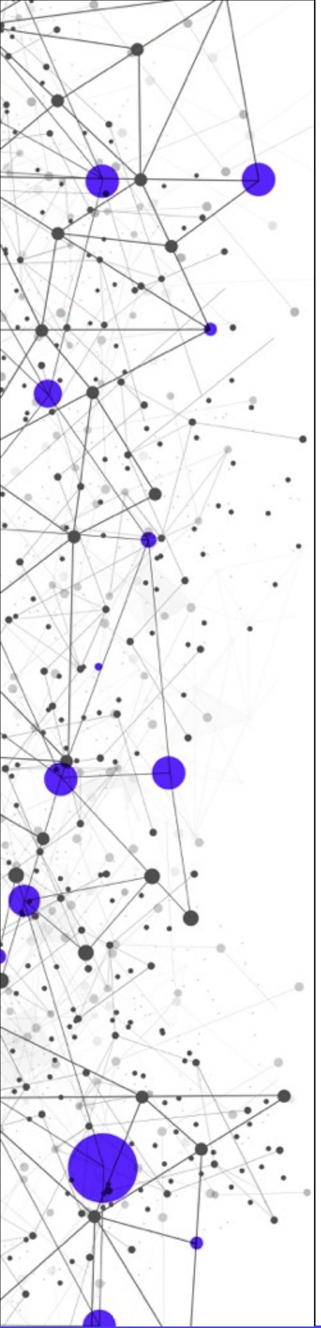
A steady level of “background noise” from low-level criminality is impacting businesses around the world.

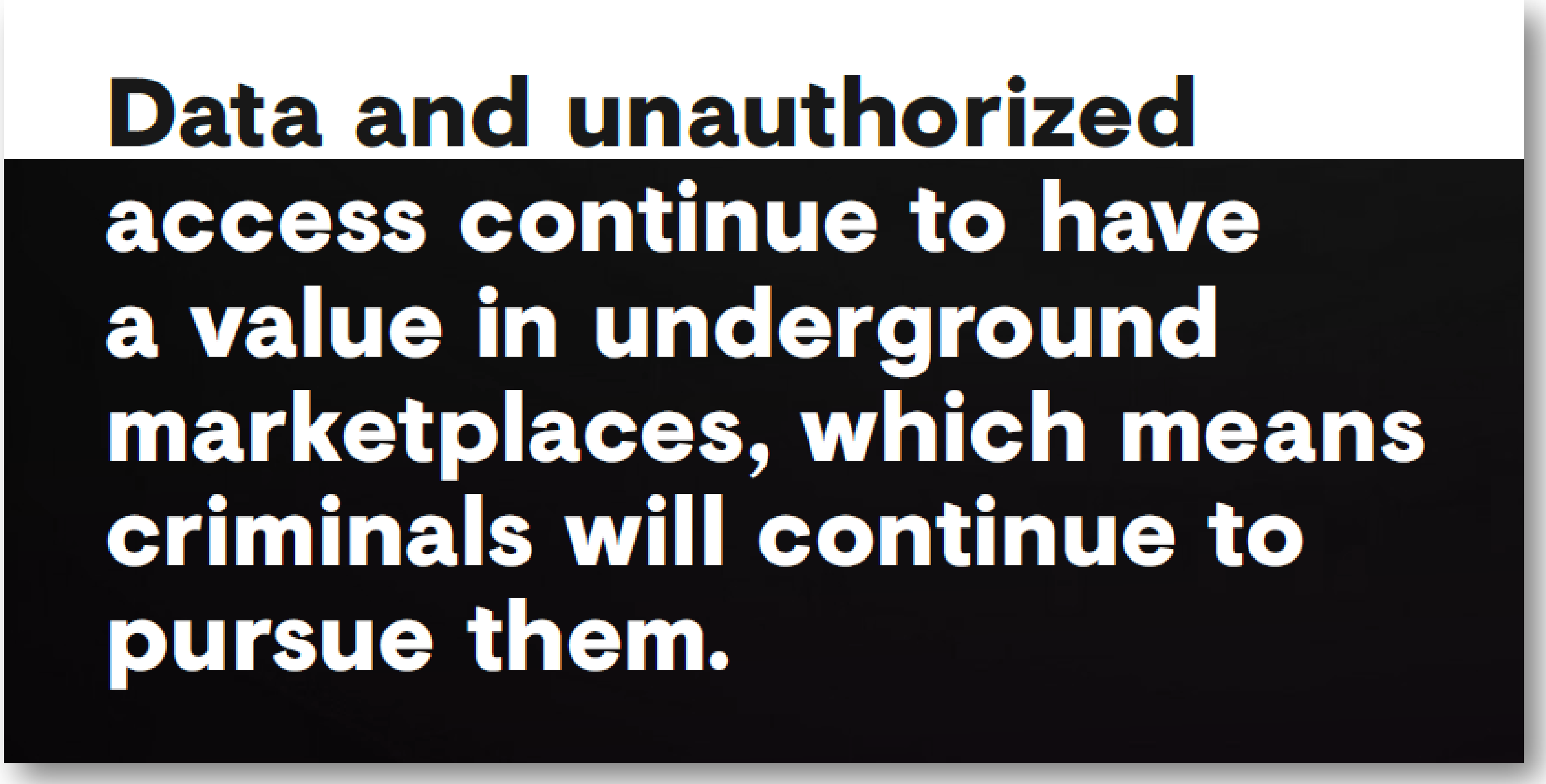


Key Learnings 1

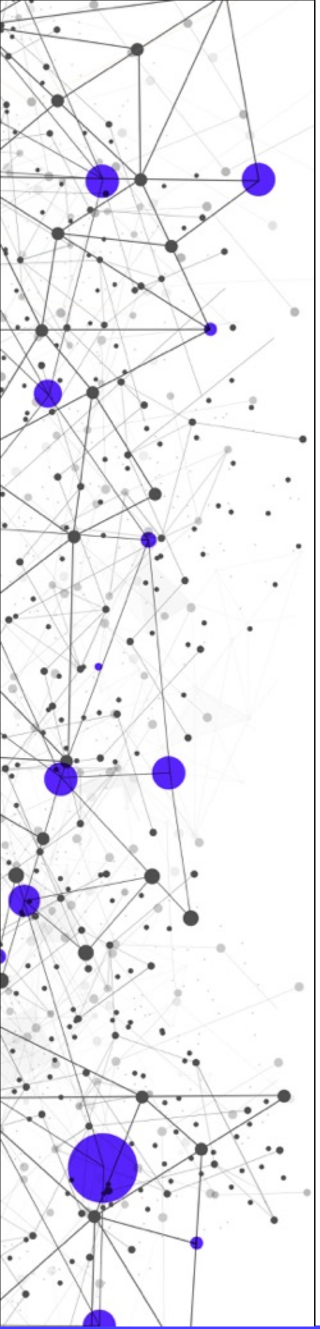
“background noise” from low level criminality is impacting businesses around the world and should not be ignored

- Cryptocurrency mining remains an extremely popular way for criminals to monetize access to infected computers.
- No significant decrease in the volume of ransomware, banking malware, point-of-sale (POS) memory scrapers or other threats available for purchase on underground forums.
- Unscrupulous hosting providers help cybercriminals stay below the radar by offering them access to anonymized servers and Internet access.
- Spam remains the leading means by which criminals deliver malware.





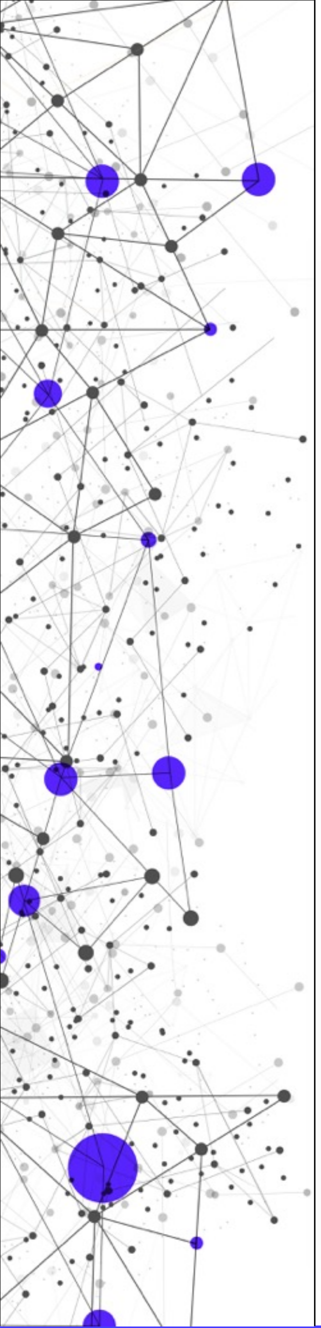
Data and unauthorized access continue to have a value in underground marketplaces, which means criminals will continue to pursue them.

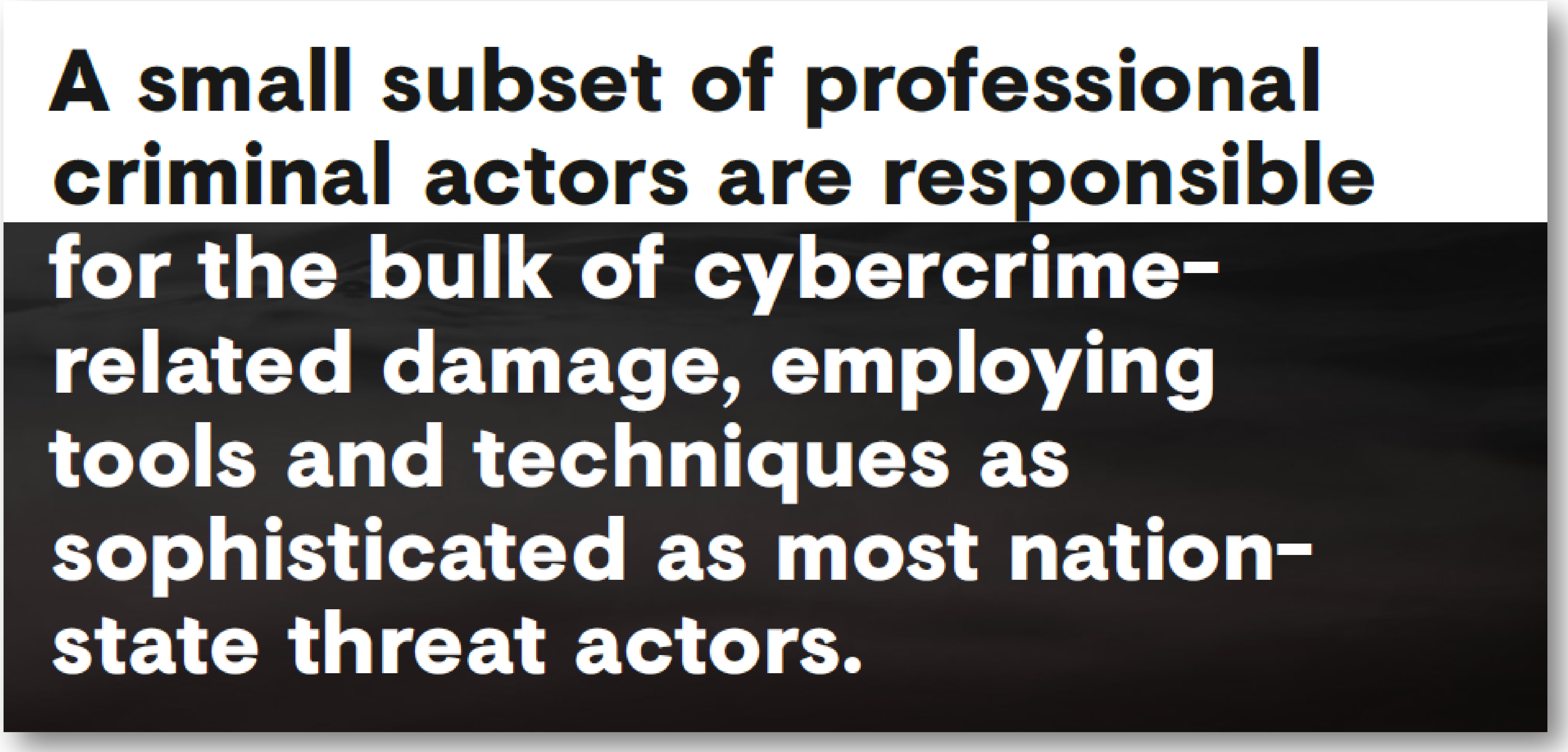


Key Learnings 2

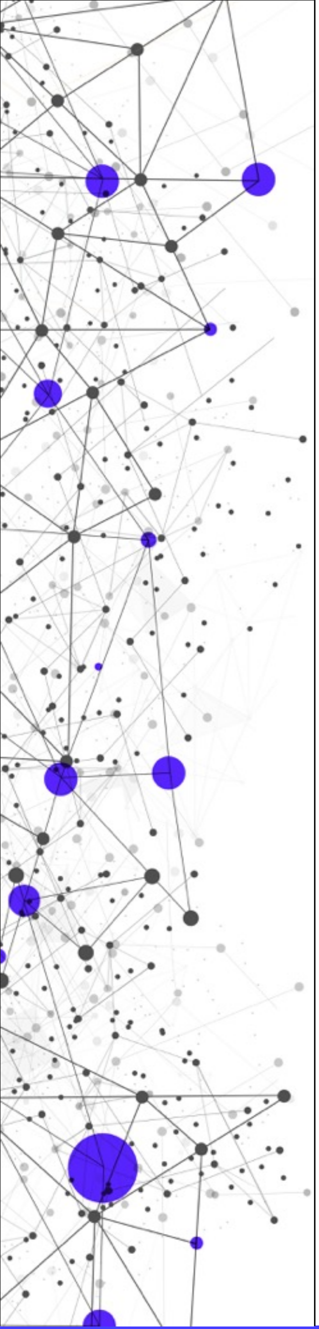
Data and unauthorized access continue to have a value in underground marketplaces, which means criminals will continue to pursue them.

- Personally identifiable information (PII), including full biographic dossiers, payment card data and other bulk data sets, are regularly offered for sale in underground forums.
- Criminals also use forums to sell access to compromised systems and organizations.





A small subset of professional criminal actors are responsible for the bulk of cybercrime-related damage, employing tools and techniques as sophisticated as most nation-state threat actors.

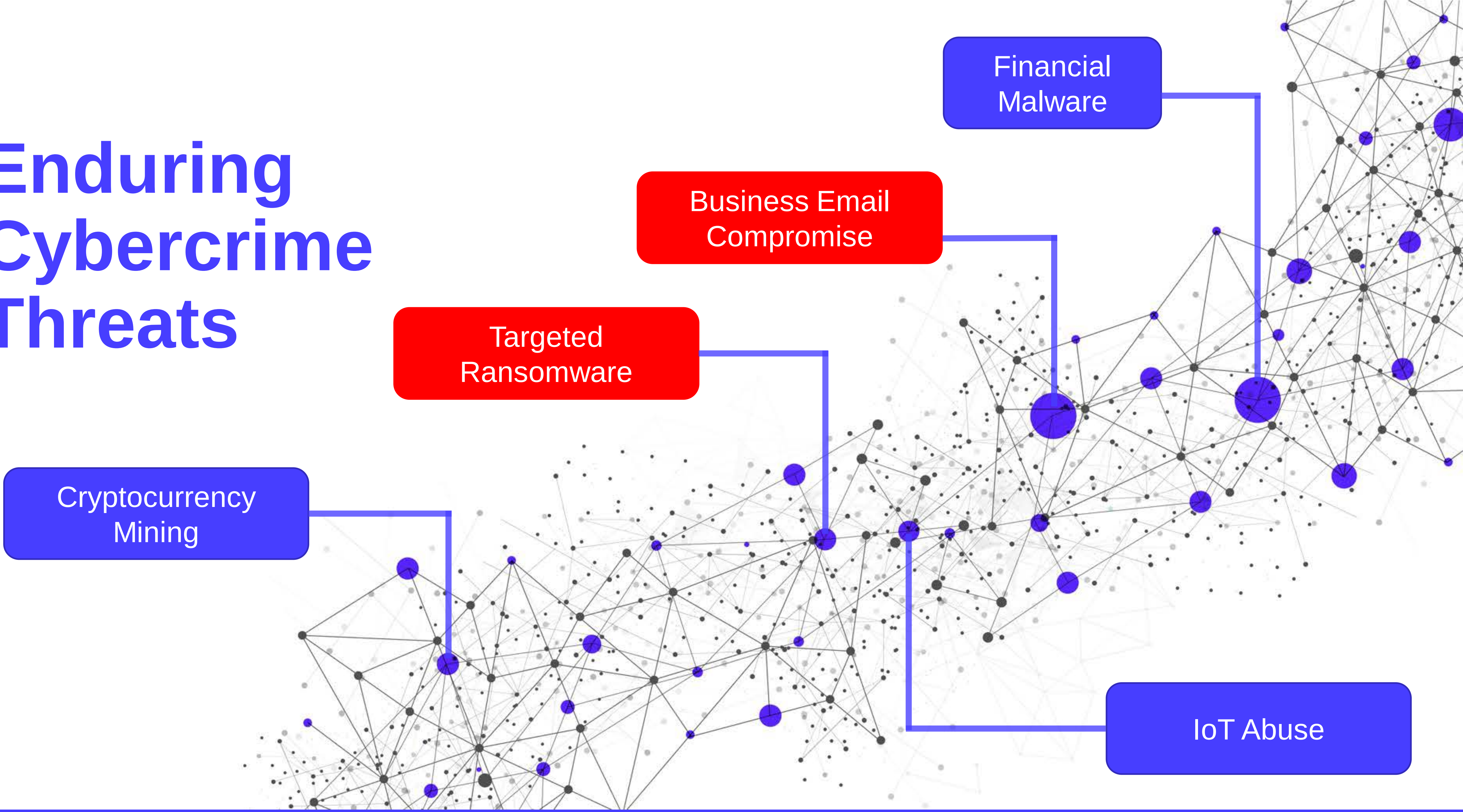


Key Learnings 3

A small subset of professional criminal actors are responsible for the bulk of cybercrime-related damage, employing tools and techniques as sophisticated as most nation-state threat actors.

- PoS Malware intrusions
- ATM jackpotting and “global cashout” operations
- Banking malware continues to evolve
- Targeted ransomware operations:
  - SamsamCrypt
  - BitPaymer
- Boundary between nation-state and cybercriminal actors continues to blur

Enduring Cybercrime Threats



Financial Malware

Business Email Compromise

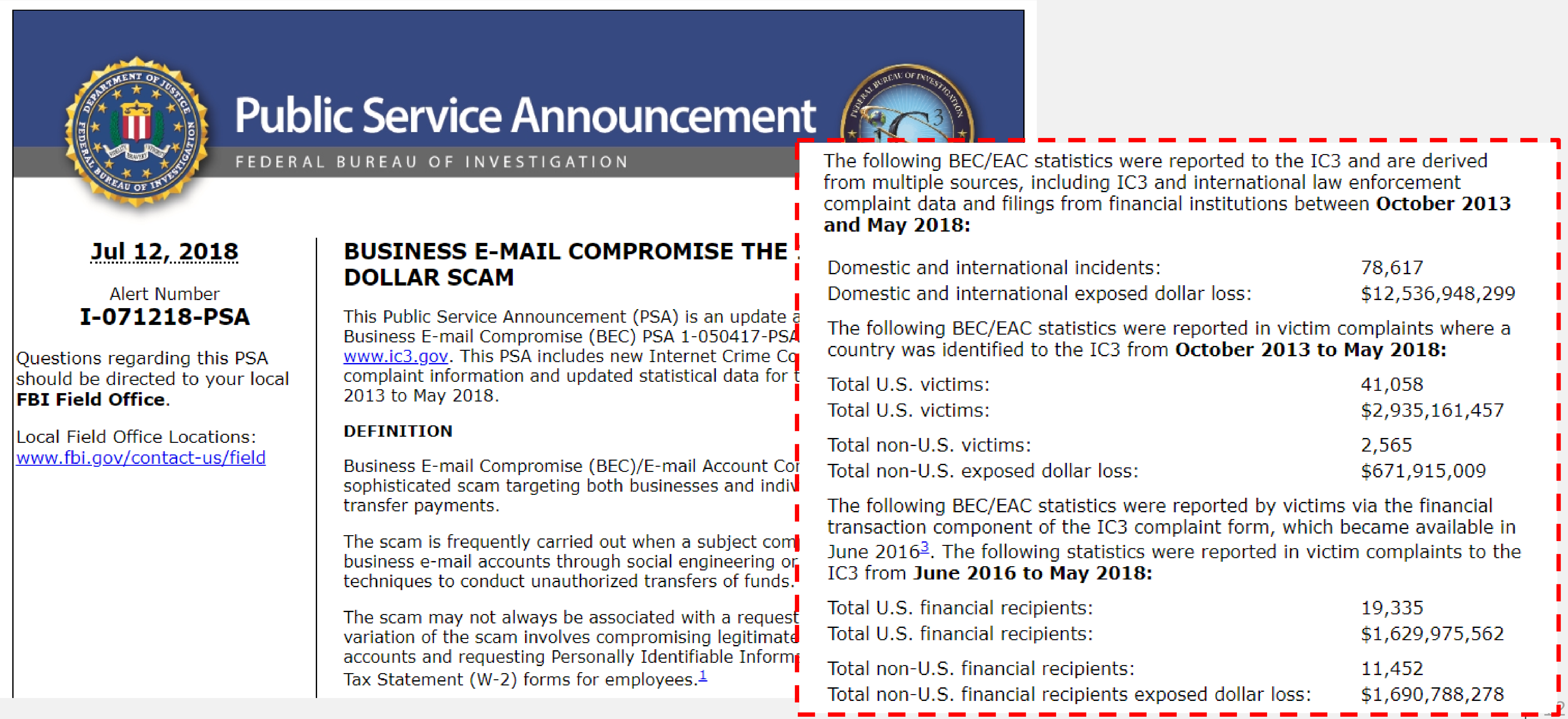
Targeted Ransomware

Cryptocurrency Mining

IoT Abuse

Business Email Compromise

“$12 BILLION” – May 2018



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number

I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE
DOLLAR SCAM

This Public Service Announcement (PSA) is an update a Business E-mail Compromise (BEC) PSA 1-050417-PSA www.ic3.gov. This PSA includes new Internet Crime Co complaint information and updated statistical data for t 2013 to May 2018.

DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Co sophisticated scam targeting both businesses and indiv transfer payments.

The scam is frequently carried out when a subject com business e-mail accounts through social engineering or techniques to conduct unauthorized transfers of funds.

The scam may not always be associated with a request variation of the scam involves compromising legitimate accounts and requesting Personally Identifiable Inform Tax Statement (W-2) forms for employees.[1]

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018:**

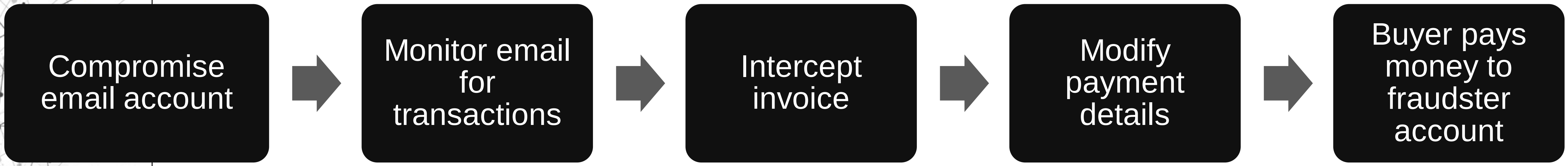
Total U.S. victims:	41,058
Total U.S. victims:	$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	$671,915,009

The following BEC/EAC statistics were reported by victims via the financial transaction component of the IC3 complaint form, which became available in June 2016[3]. The following statistics were reported in victim complaints to the IC3 from **June 2016 to May 2018:**

Total U.S. financial recipients:	19,335
Total U.S. financial recipients:	$1,629,975,562
Total non-U.S. financial recipients:	11,452
Total non-U.S. financial recipients exposed dollar loss:	$1,690,788,278

How does BEC work?

High level overview



Compromise email account → Monitor email for transactions → Intercept invoice → Modify payment details → Buyer pays money to fraudster account

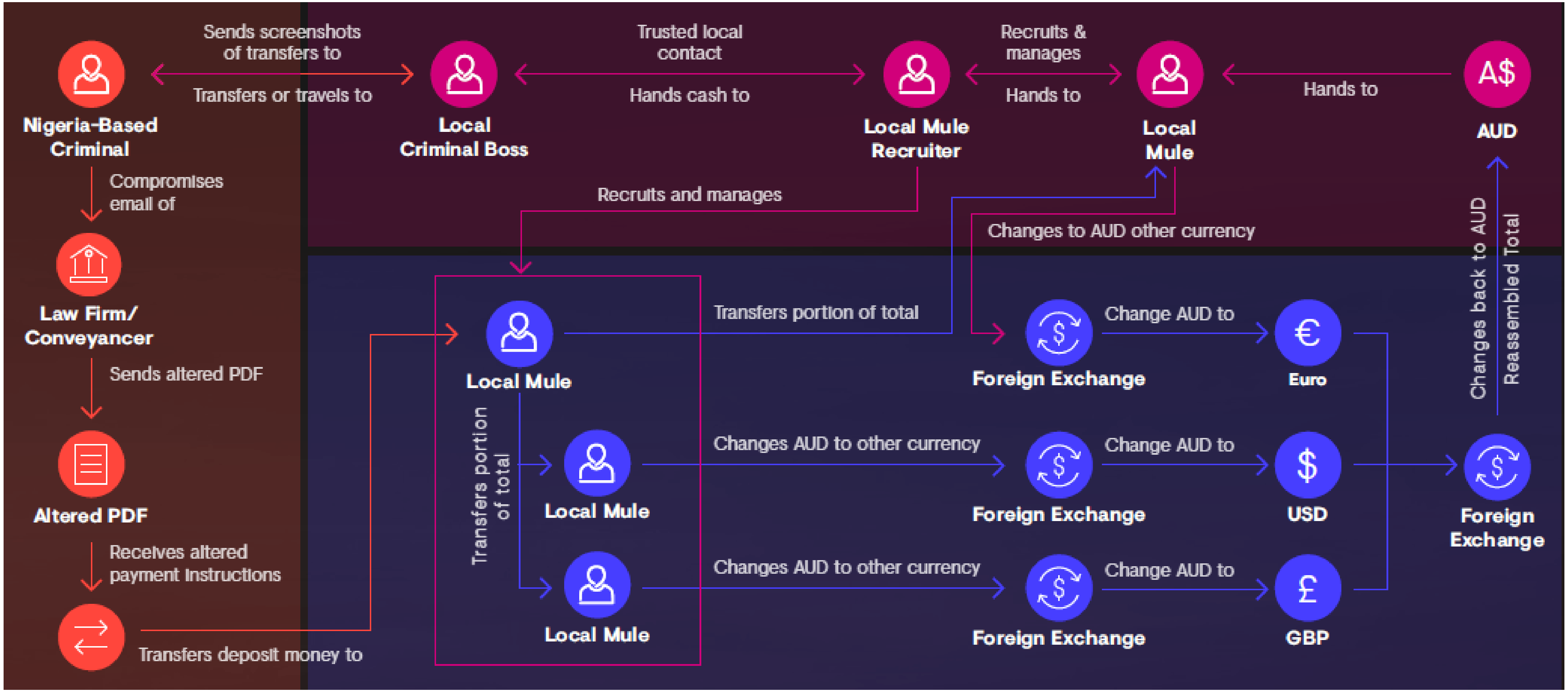
Commonly Impacts:

- Real Estate
- Shipping
- Manufacturing
- Aviation
- Retail
- Law firms

But lots of other variants exist

Business Email Compromise

GOLD MILTON

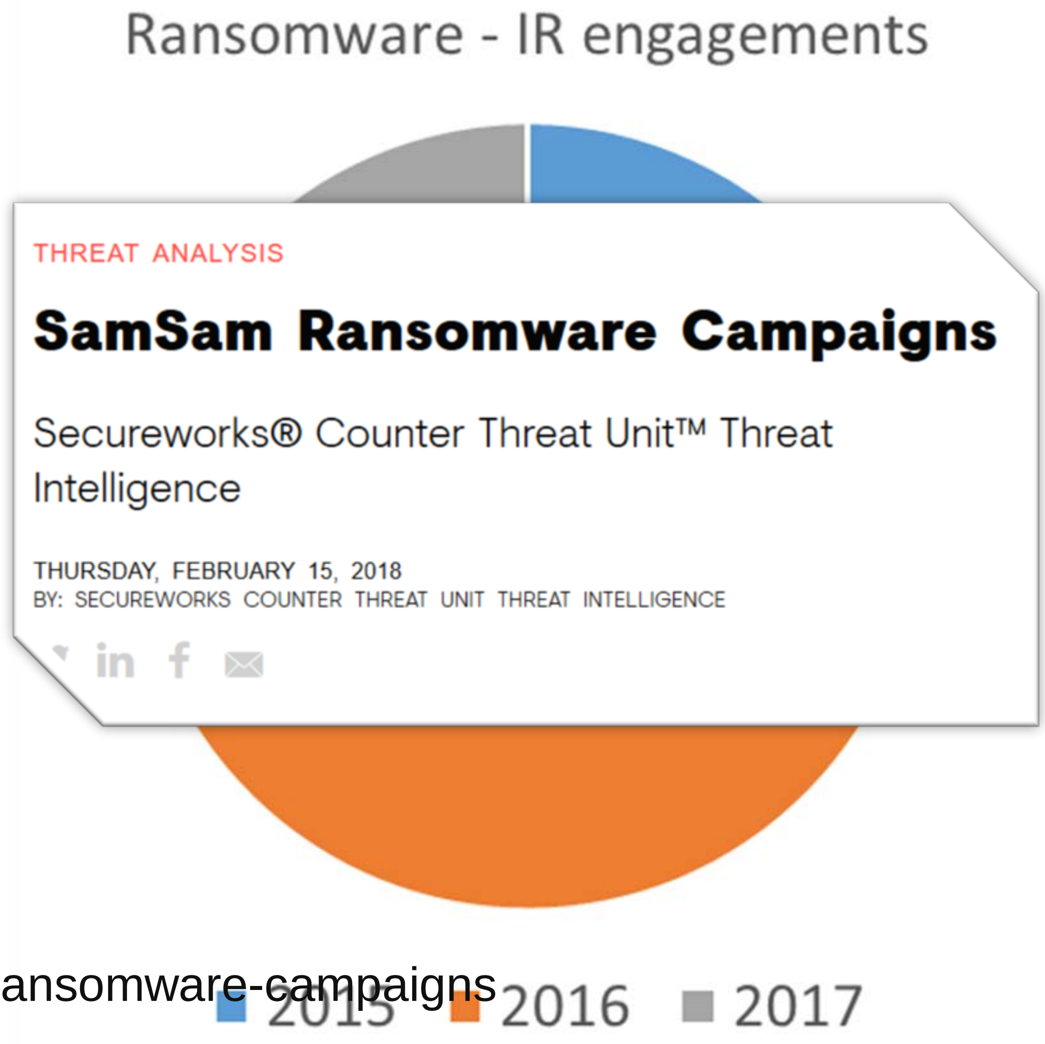


Targeted Ransomware

Is ransomware use reducing?

Possibly…

- Criminals are business oriented
- Organisations are better prepared
- Still a major threat to unprepared organisations
- GOLD LOWELL is having a lot of success with targeted Ransomware attacks using SamSam Crypt.



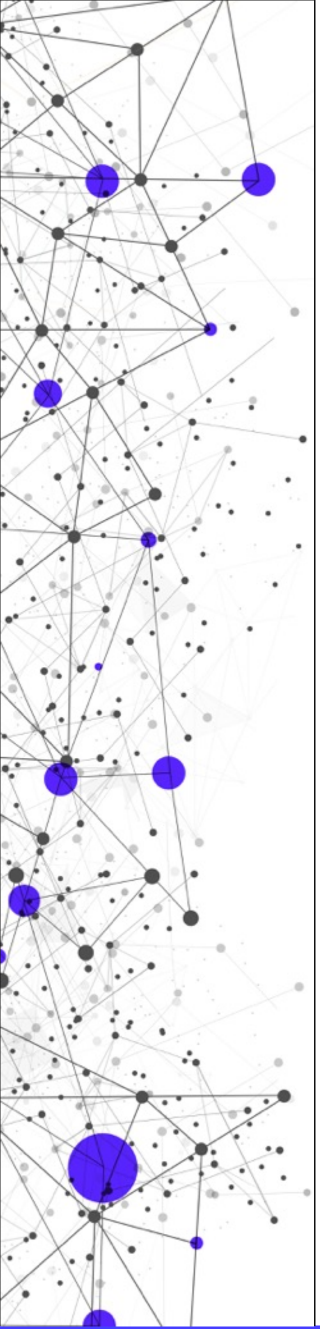
THREAT ANALYSIS

SamSam Ransomware Campaigns

Secureworks® Counter Threat Unit™ Threat Intelligence

THURSDAY, FEBRUARY 15, 2018
BY: SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

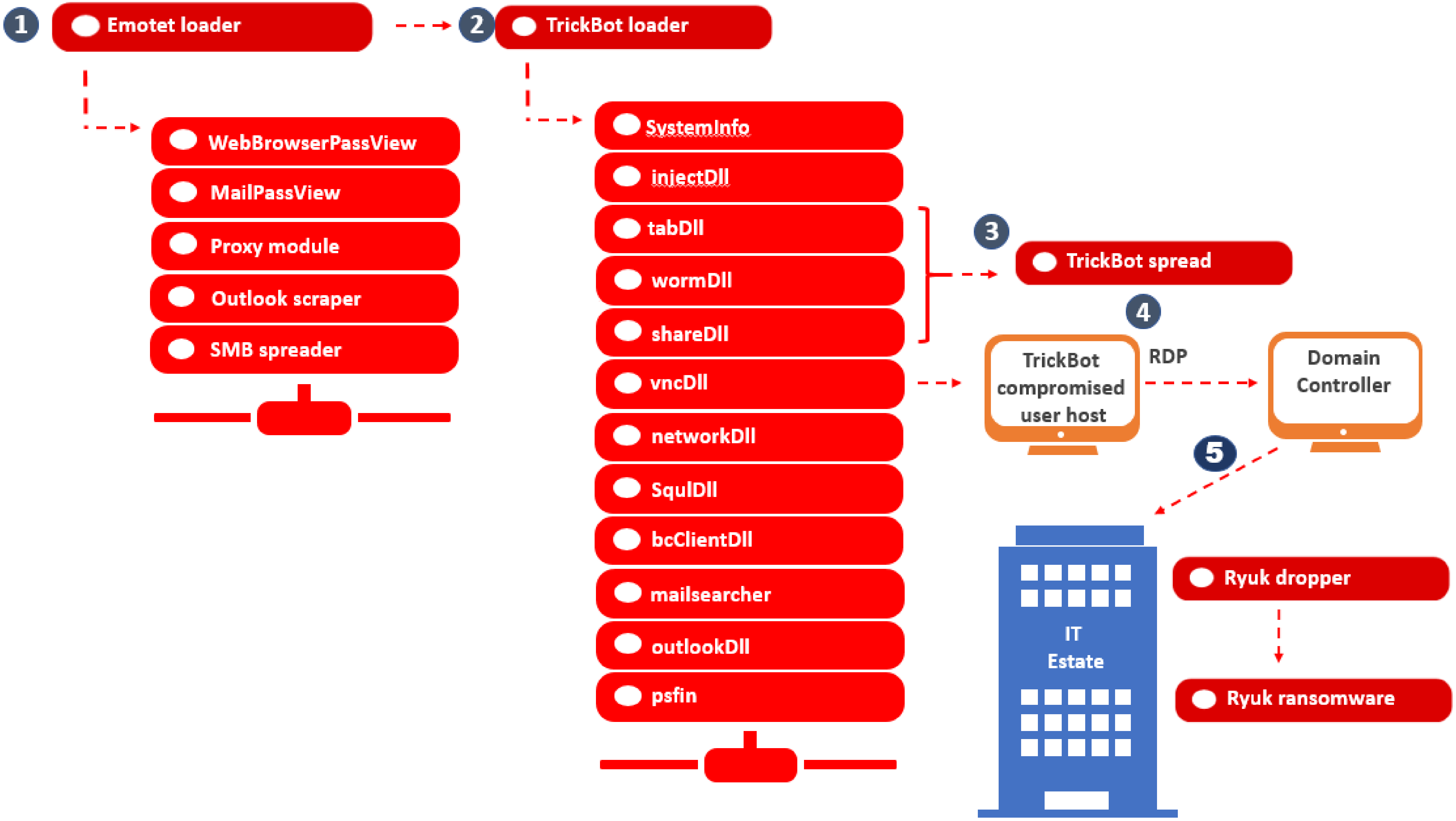
https://www.secureworks.com/research/samsam-ransomware-campaigns



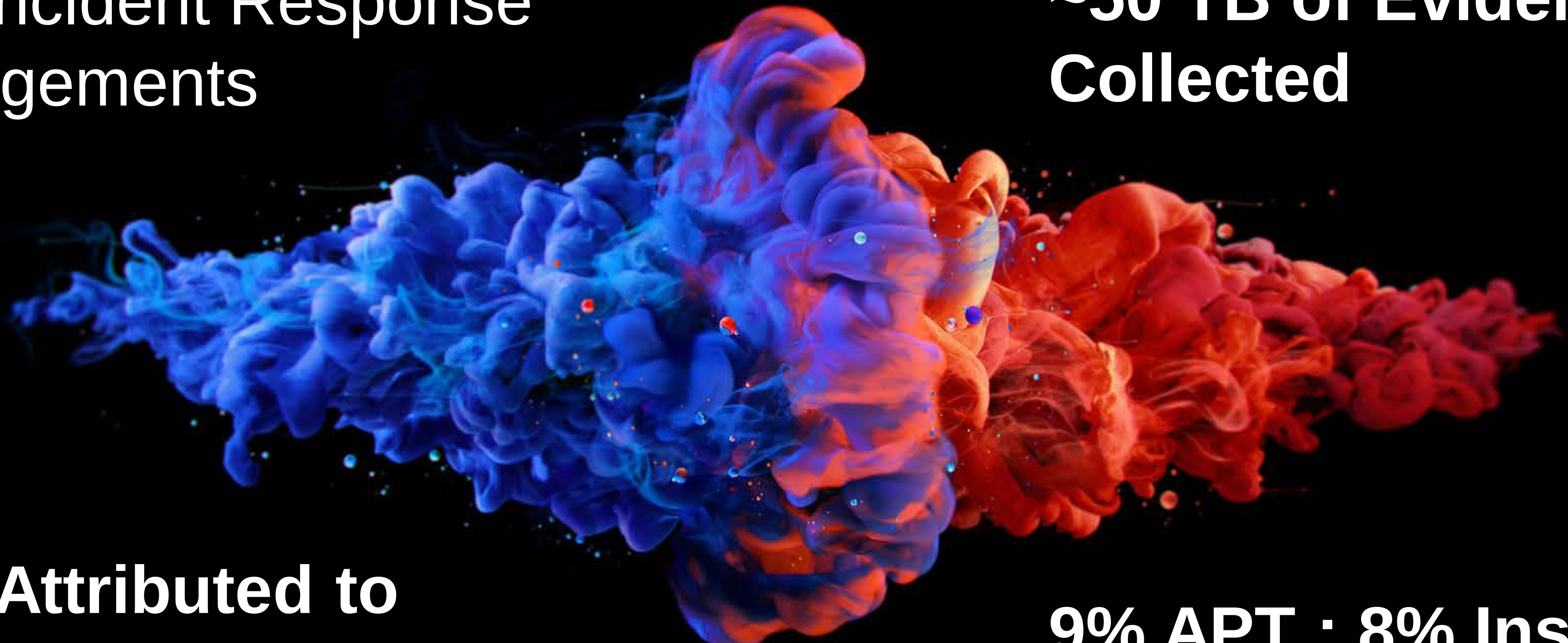
Targeted ransomware still highly effective

Organisations are more likely to pay if a significant percentage of their business is affected.

- **Targeted Ransomware Examples:**
  - **SamSam Crypt**
  - **Bitpaymer**
  - **Ryuk / Hermes**


1
Emotet loader
2
TrickBot loader
WebBrowserPassView
MailPassView
Proxy module
Outlook scraper
SMB spreader
SystemInfo
injectDll
tabDll
wormDll
shareDll
vncDll
networkDll
SqulDll
bcClientDll
mailsearcher
outlookDll
psfin
3
TrickBot spread
4
TrickBot compromised user host
RDP
Domain Controller
5
IT Estate
Ryuk dropper
Ryuk ransomware

2018 IR Insights Report



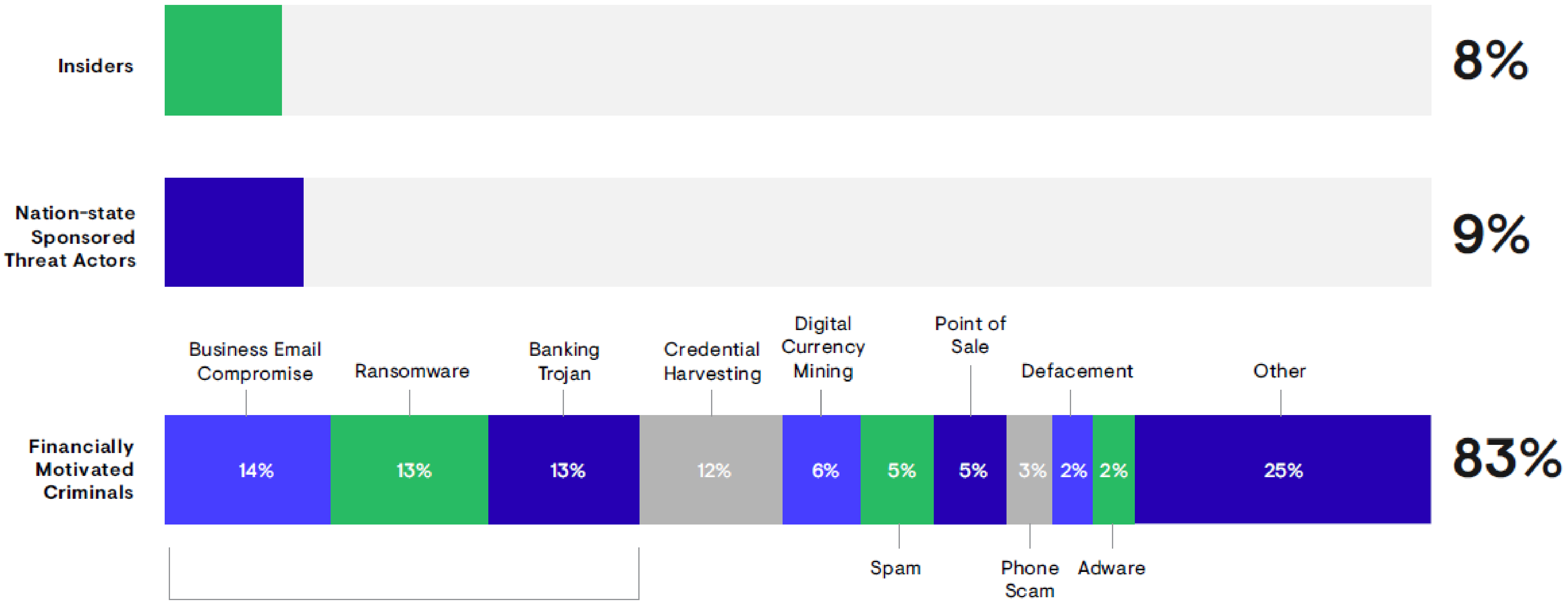
996 Incident Response Engagements

~50 TB of Evidence Collected

83% Attributed to Criminal Activity

9% APT : 8% Insider

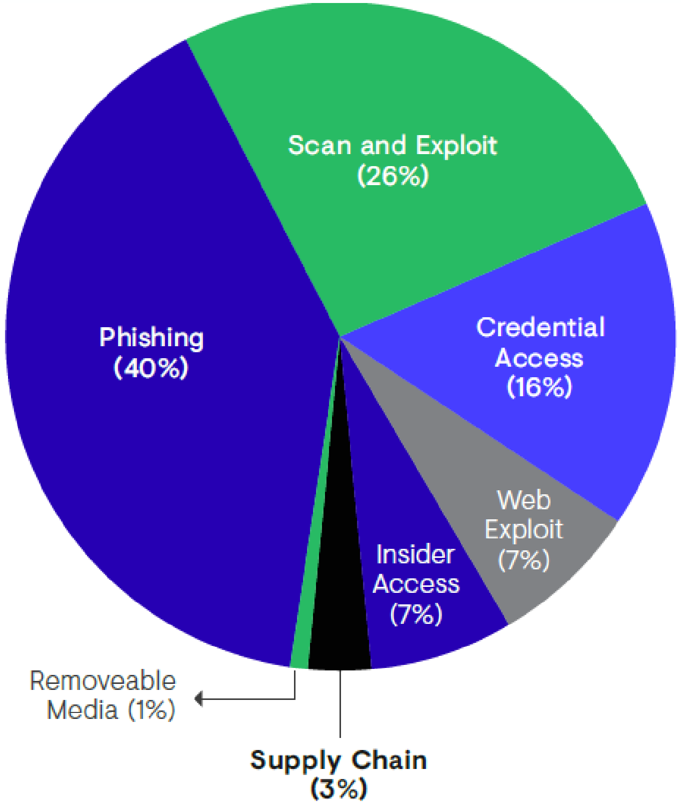
A Global Profile of Threats



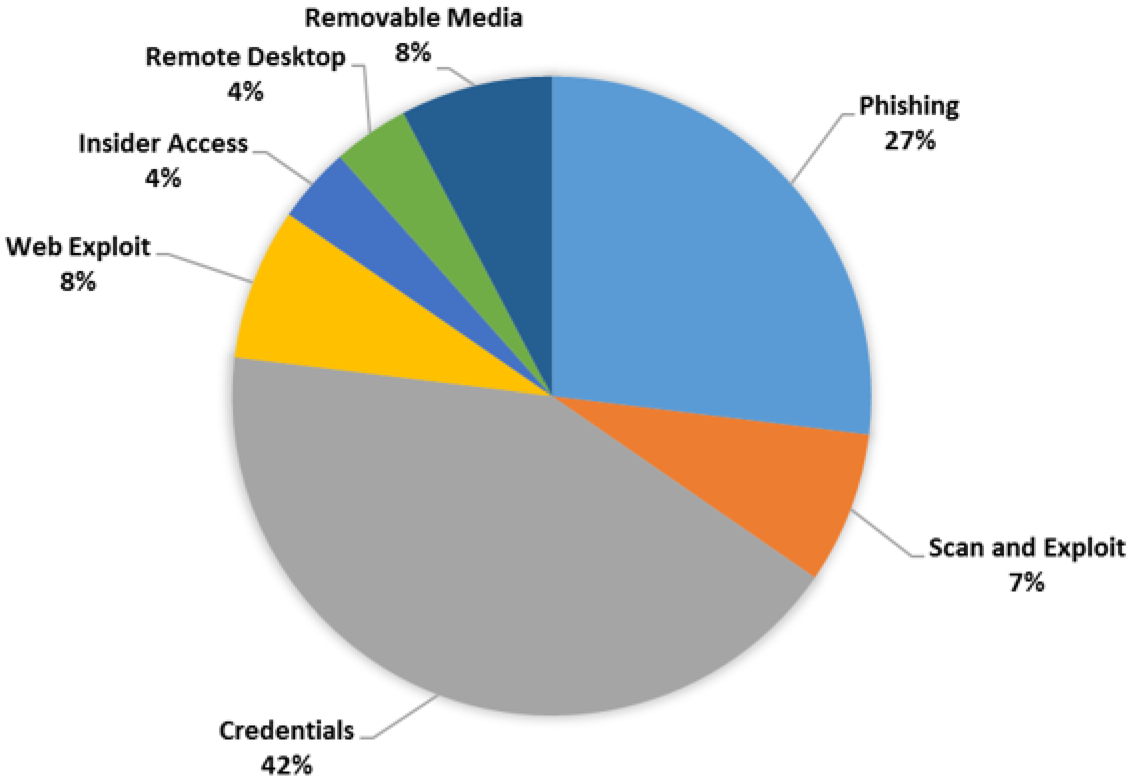
Together, **Business Email Compromise, Ransomware**, and **Banking Trojans** accounted for 1/3 of all incidents Secureworks supported in 2017

How Attackers Gained Entry

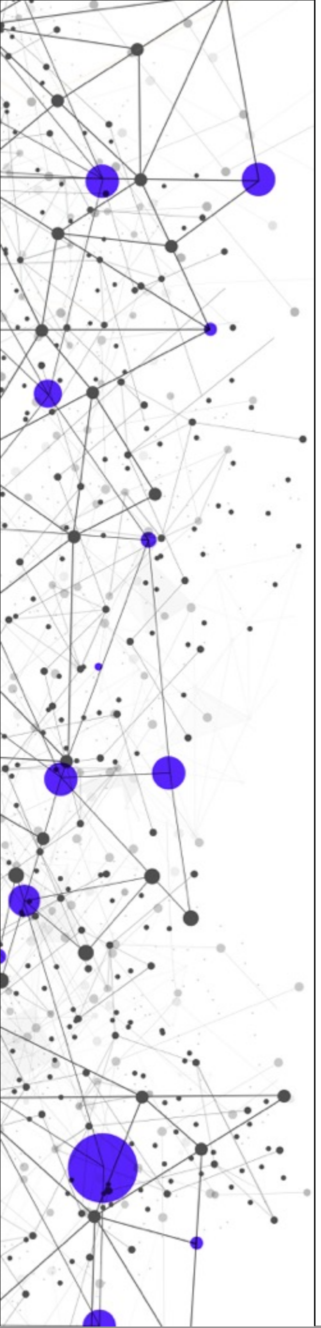
2017 vs 2018 (interim results)



2017: 12 Months



2018: July - September



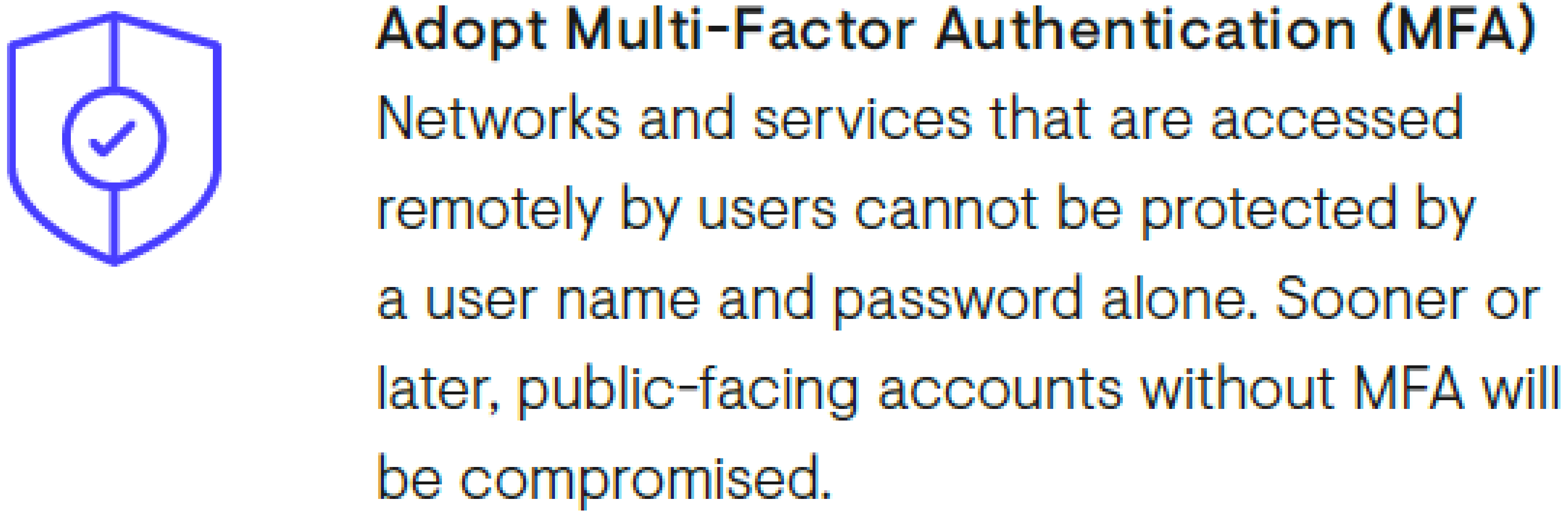
Patch > Vulnerability Management > Zero Day

Prioritise efforts based on real world intelligence

“The idea that attacks are routinely leveraging zeroday vulnerabilities which defenders are powerless to prevent is a myth.

In almost every case where software vulnerabilities were exploited to gain access to a network or system, the vendor had released security patches for those vulnerabilities months beforehand.”

Top 5 Control Recommendations



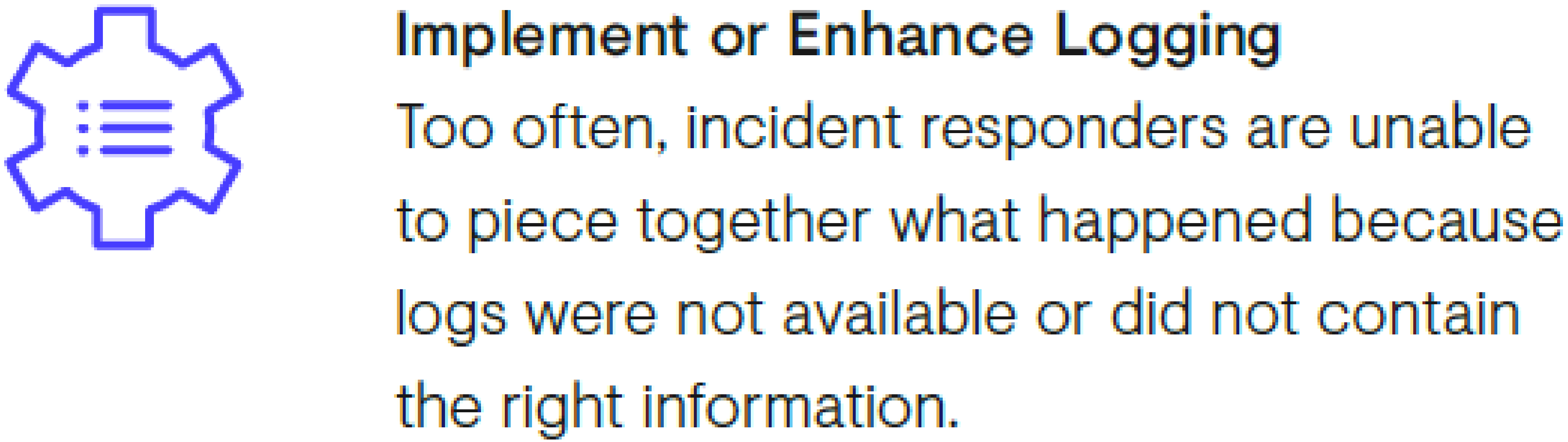
Adopt Multi-Factor Authentication (MFA)

Networks and services that are accessed remotely by users cannot be protected by a user name and password alone. Sooner or later, public-facing accounts without MFA will be compromised.

Critical for:

- Reducing the impact of credential theft during an intrusion
- Mitigating or reducing the risk of Business Email Compromise (BEC) fraud to the business
- Mitigating or reducing the impact of Password Spraying attacks

TIP: If you use an SMS token based solution, consider transitioning to hard or soft tokens. SMS tokens are increasingly prone to capture at the ISP level or via SIM swap attacks.

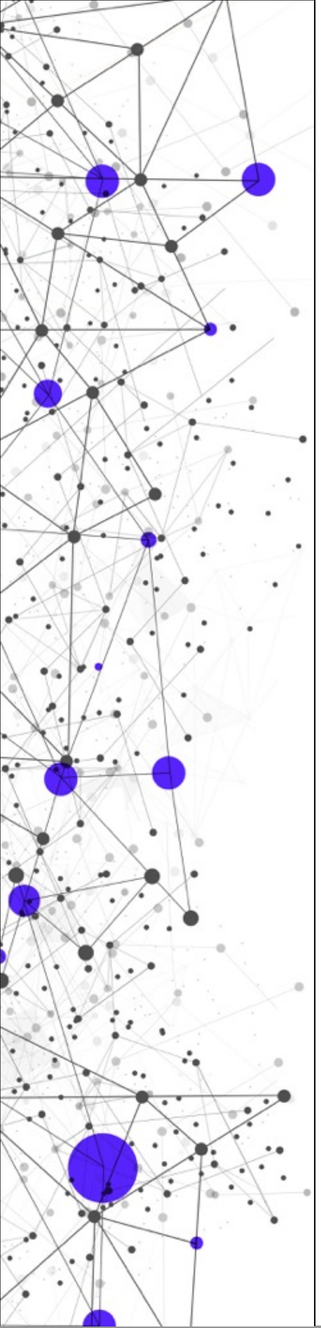


Implement or Enhance Logging

Too often, incident responders are unable to piece together what happened because logs were not available or did not contain the right information.

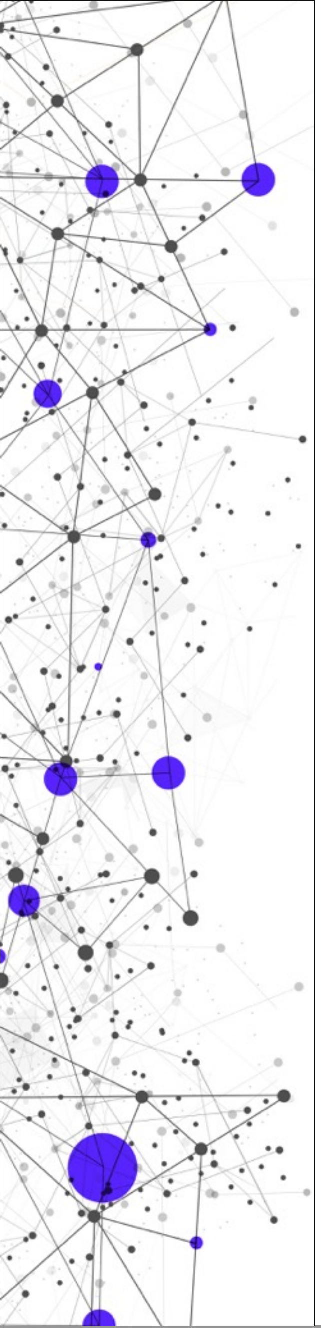
Critical for:

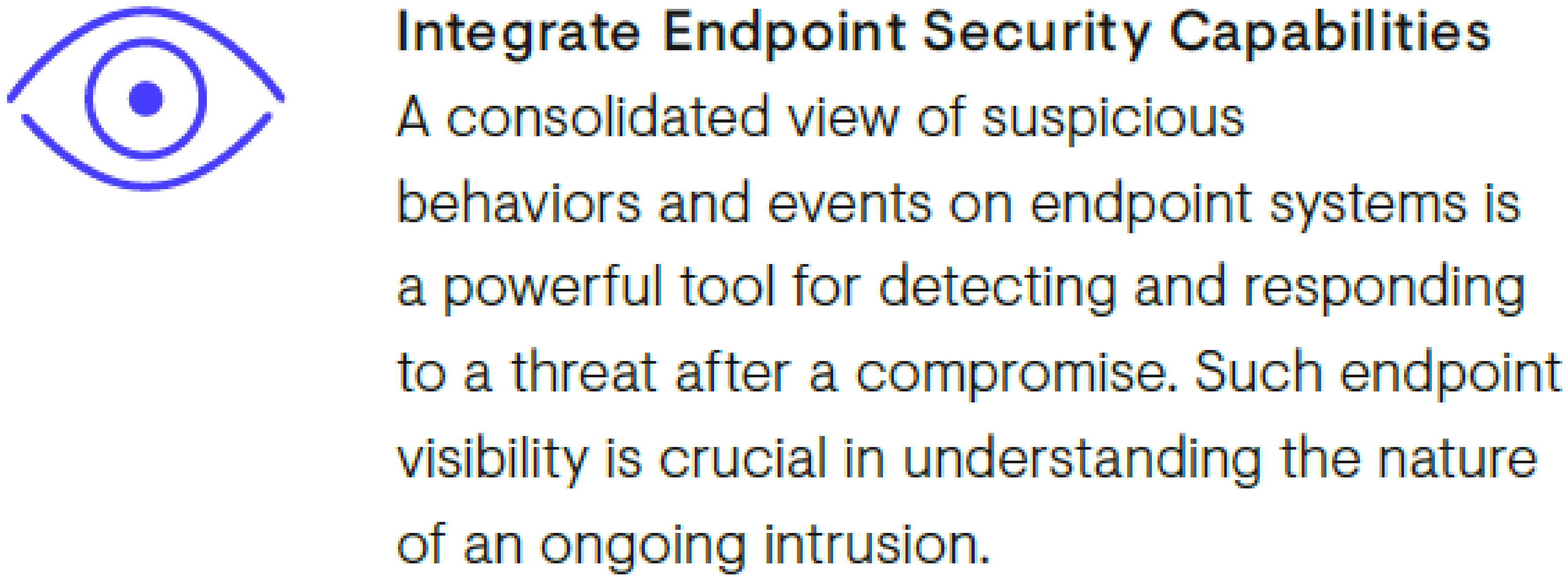
- Early detection, reducing adversary dwell time
- Understand the scope of the breach
- Determine initial access vector
- Determine compromised accounts



Manage User Account Privileges

Attackers routinely exploit redundant accounts or accounts with unnecessary access rights to obtain more privileges in a compromised network. They often target administrative access on end user systems to gain an initial foothold.

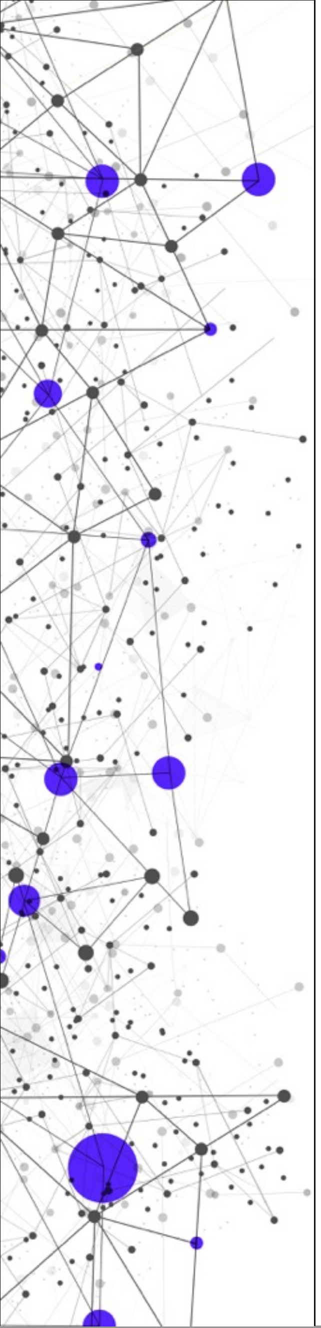




Integrate Endpoint Security Capabilities

A consolidated view of suspicious behaviors and events on endpoint systems is a powerful tool for detecting and responding to a threat after a compromise. Such endpoint visibility is crucial in understanding the nature of an ongoing intrusion.

- Critical for:
  - Early detection, reducing adversary dwell time
  - High context record of activity
  - Like CCTV for your End-Point estate



Develop or Practice Incident Response Planning

Responding to incidents effectively is difficult without the right preparation. Organizations are more resilient when tried and tested response plans are in place.

Thank You