HUNTRESS

The Cyber Landscape and How Huntress Fights Back

> whoami

- Born and raised in Bronx, NY
- US Army Veteran (1998-2007)
- Worked at DOD, Carbon Black and Red Canary
- Background in technical training and network management
- Bachelors of Science, IT from Western Governors University
- Proud Husband and Dad (2 adult sons, 1 adolescent daughter, and 2 Frenchies)

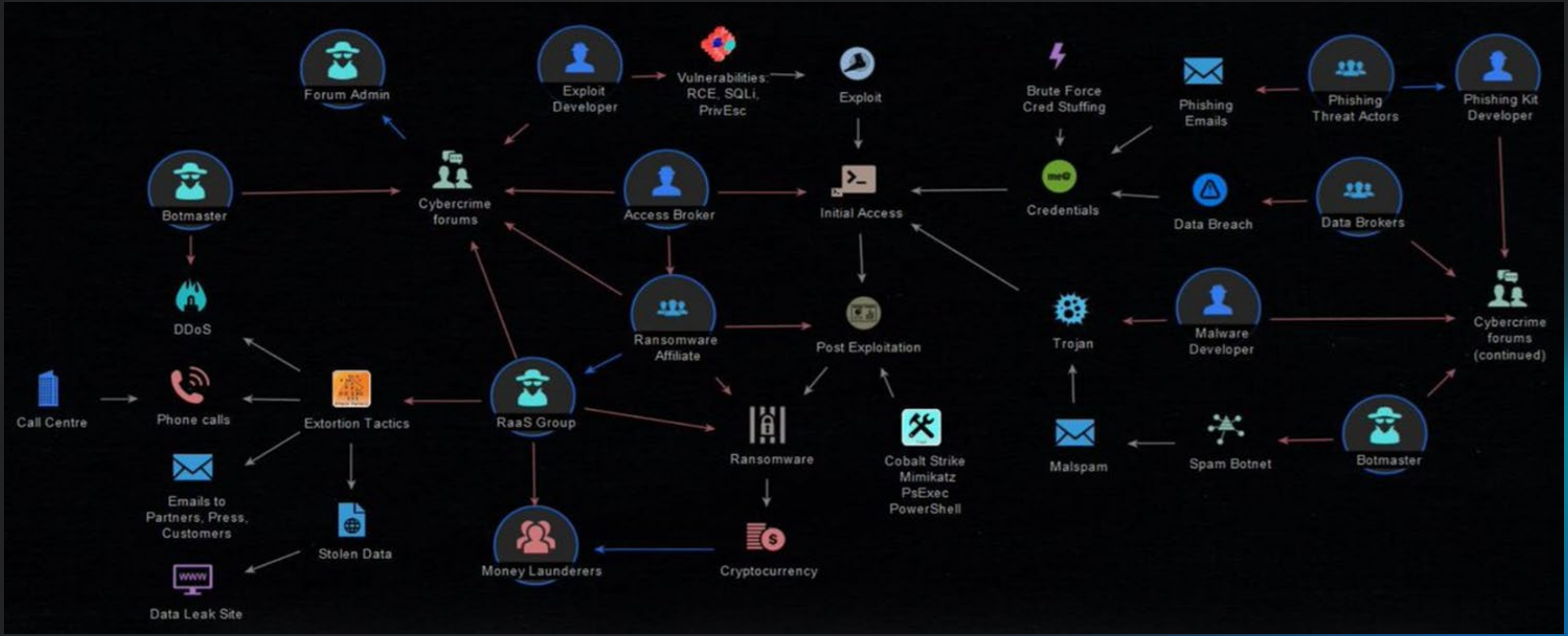
Jimmy Colvin
Huntress
Technical Account Manager

MYTH:

Hackers are nerds who wear hooded sweatshirts and write code in their moms' basements.

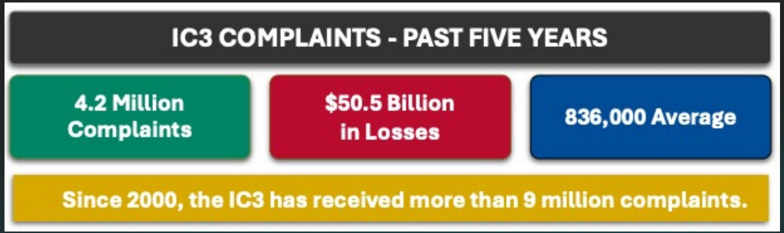
Cybercriminals Earn Money All Sorts of Ways

The evolution of the industry is towards specialization and monetization.



Hacking is a Business

Cybercrime is a booming industry!



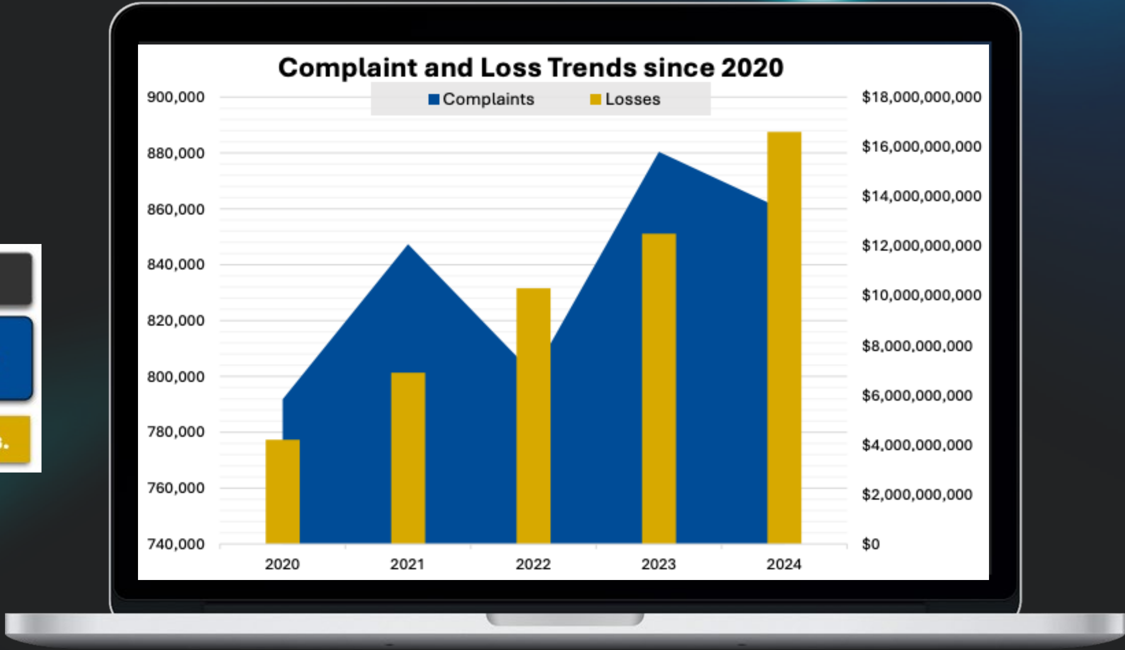
IC3 COMPLAINTS - PAST FIVE YEARS

4.2 Million Complaints

$50.5 Billion in Losses

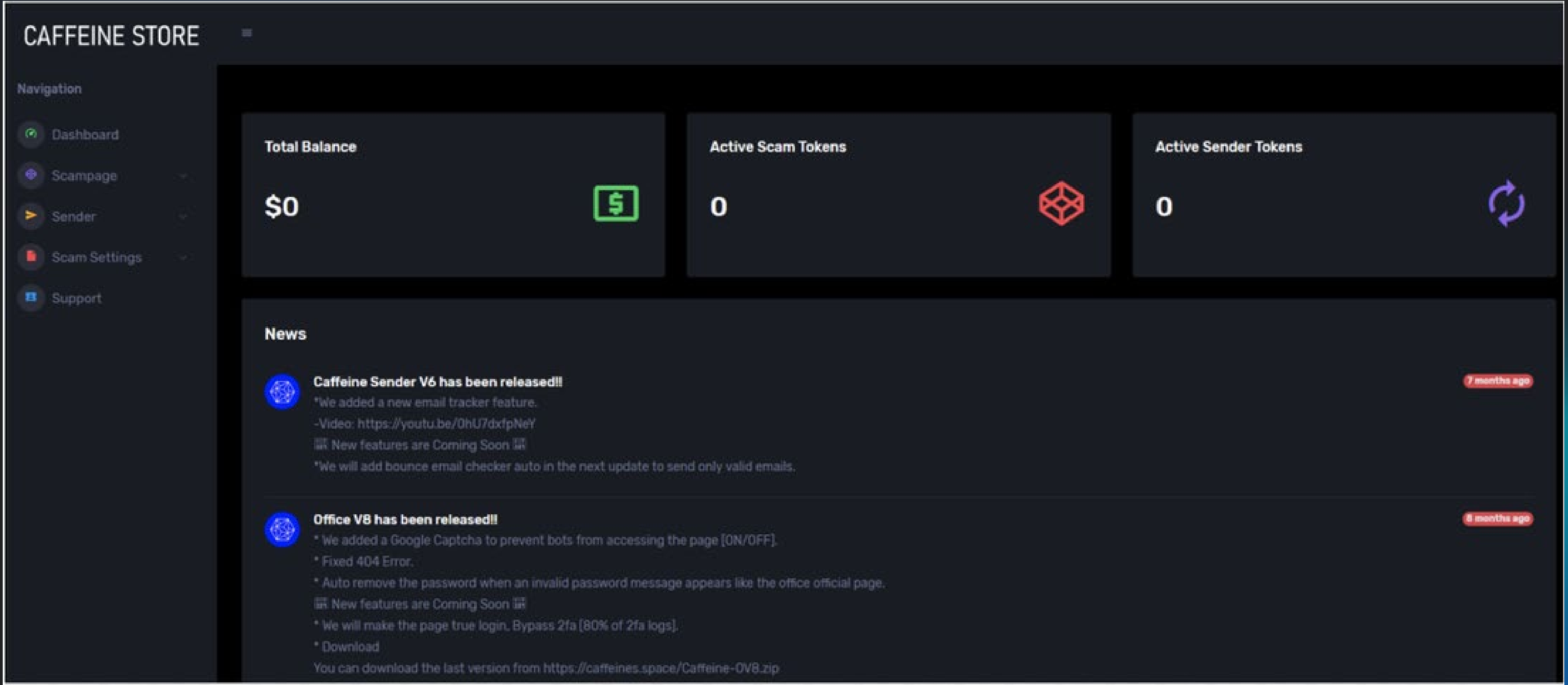
836,000 Average

Since 2000, the IC3 has received more than 9 million complaints.



SOURCE: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Phishing as a Service (PhaaS)



Total Balance
$0

Active Scam Tokens
0

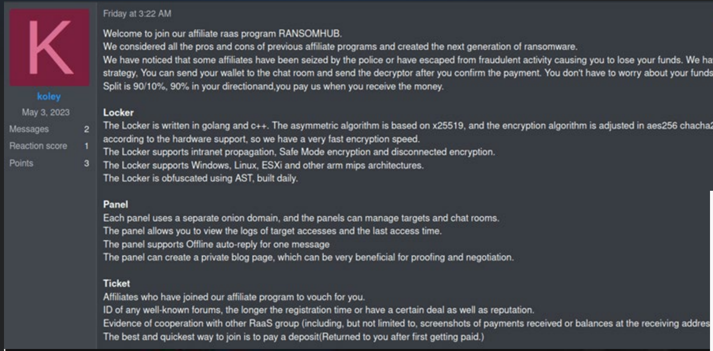
Active Sender Tokens
0

News

Caffeine Sender V6 has been released!! 7 months ago
*We added a new email tracker feature.
-Video: https://youtu.be/0hU7dxfpNeY
🆕 New features are Coming Soon 🆕
*We will add bounce email checker auto in the next update to send only valid emails.

Office V8 has been released!! 8 months ago
* We added a Google Captcha to prevent bots from accessing the page [ON/OFF].
* Fixed 404 Error.
* Auto remove the password when an invalid password message appears like the office official page.
🆕 New features are Coming Soon 🆕
* We will make the page true login. Bypass 2fa [80% of 2fa logs].
* Download
You can download the last version from https://caffeines.space/Caffeine-OV8.zip

Ransomware as a Service (RaaS)



koley
May 3, 2023
Messages 2
Reaction score 1
Points 3

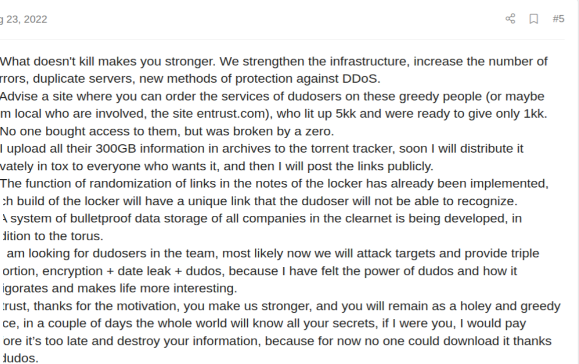
Friday at 3:22 AM New #1

Welcome to join our affiliate raas program RANSOMHUB.
We considered all the pros and cons of previous affiliate programs and created the next generation of ransomware.
We have noticed that some affiliates have been seized by the police or have escaped from fraudulent activity causing you to lose your funds. We have adopted a new strategy, You can send your wallet to the chat room and send the decryptor after you confirm the payment. You don't have to worry about your funds security.
Split is 90/10%, 90% in your directionand,you pay us when you receive the money.

Locker
The Locker is written in golang and c++. The asymmetric algorithm is based on x25519, and the encryption algorithm is adjusted in aes256 chacha20 xchacha20 according to the hardware support, so we have a very fast encryption speed.
The Locker supports intranet propagation, Safe Mode encryption and disconnected encryption.
The Locker supports Windows, Linux, ESXi and other arm mips architectures.
The Locker is obfuscated using AST, built daily.

Panel
Each panel uses a separate onion domain, and the panels can manage targets and chat rooms.
The panel allows you to view the logs of target accesses and the last access time.
The panel supports Offline auto-reply for one message
The panel can create a private blog page, which can be very beneficial for proofing and negotiation.

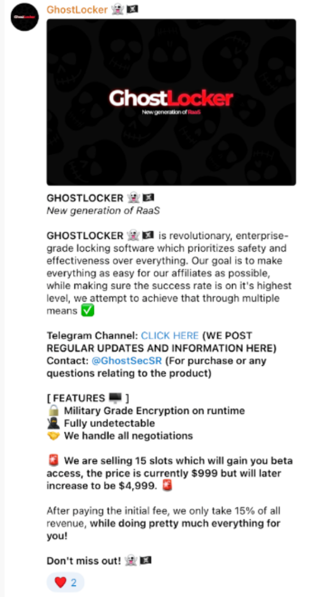
Ticket
Affiliates who have joined our affiliate program to vouch for you.
ID of any well-known forums, the longer the registration time or have a certain deal as well as reputation.
Evidence of cooperation with other RaaS group (including, but not limited to, screenshots of payments received or balances at the receiving addres
The best and quickest way to join is to pay a deposit(Returned to you after first getting paid.)



LOCKBIT
LockBitSupp
Premium
Premium
Joined: Mar 8, 2021
Messages: 539
Reaction score: 1,120

Aug 23, 2022 #5

1. What doesn't kill makes you stronger. We strengthen the infrastructure, increase the number of mirrors, duplicate servers, new methods of protection against DDoS.
2. Advise a site where you can order the services of dudosers on these greedy people (or maybe from local who are involved, the site entrust.com), who lit up 5kk and were ready to give only 1kk.
3. No one bought access to them, but was broken by a zero.
4. I upload all their 300GB information in archives to the torrent tracker, soon I will distribute it privately in tox to everyone who wants it, and then I will post the links publicly.
5. The function of randomization of links in the notes of the locker has already been implemented,
ch build of the locker will have a unique link that the dudoser will not be able to recognize.
A system of bulletproof data storage of all companies in the clearnet is being developed, in
dition to the torus.
am looking for dudosers in the team, most likely now we will attack targets and provide triple
ortion, encryption + date leak + dudos, because I have felt the power of dudos and how it
igorates and makes life more interesting.
rust, thanks for the motivation, you make us stronger, and you will remain as a holey and greedy
ce, in a couple of days the whole world will know all your secrets, if I were you, I would pay
ore it's too late and destroy your information, because for now no one could download it thanks
dudos.



GhostLocker 👻🏴‍☠️

GHOSTLOCKER 👻🏴‍☠️
New generation of RaaS

GHOSTLOCKER 👻🏴‍☠️ is revolutionary, enterprise-grade locking software which prioritizes safety and effectiveness over everything. Our goal is to make everything as easy for our affiliates as possible, while making sure the success rate is on it's highest level, we attempt to achieve that through multiple means ✅

Telegram Channel: CLICK HERE **(WE POST REGULAR UPDATES AND INFORMATION HERE)**
Contact: @GhostSecSR **(For purchase or any questions relating to the product)**

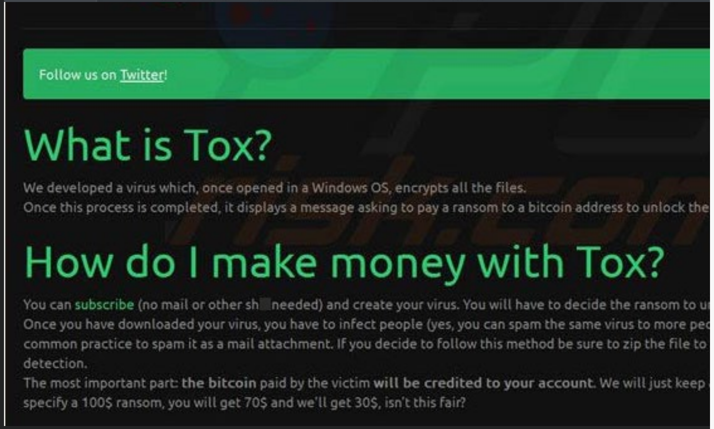
[FEATURES 🖥️]
🔒 **Military Grade Encryption on runtime**
🥷 **Fully undetectable**
🤝 **We handle all negotiations**

🚨 **We are selling 15 slots which will gain you beta access, the price is currently $999 but will later increase to be $4,999.** 🚨

After paying the initial fee, we only take 15% of all revenue, **while doing pretty much everything for you!**

Don't miss out! 👻🏴‍☠️

❤️ 2



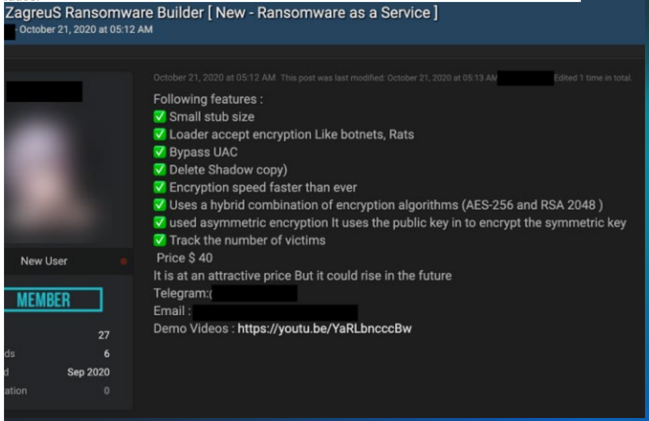
Follow us on Twitter!

What is Tox?

We developed a virus which, once opened in a Windows OS, encrypts all the files.
Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the

How do I make money with Tox?

You can subscribe (no mail or other sh[redacted]needed) and create your virus. You will have to decide the ransom to u
Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more peo
common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to
detection.
The most important part: **the bitcoin** paid by the victim **will be credited to your account.** We will just keep
specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?



ZagreuS Ransomware Builder [New - Ransomware as a Service]
[redacted] · October 21, 2020 at 05:12 AM

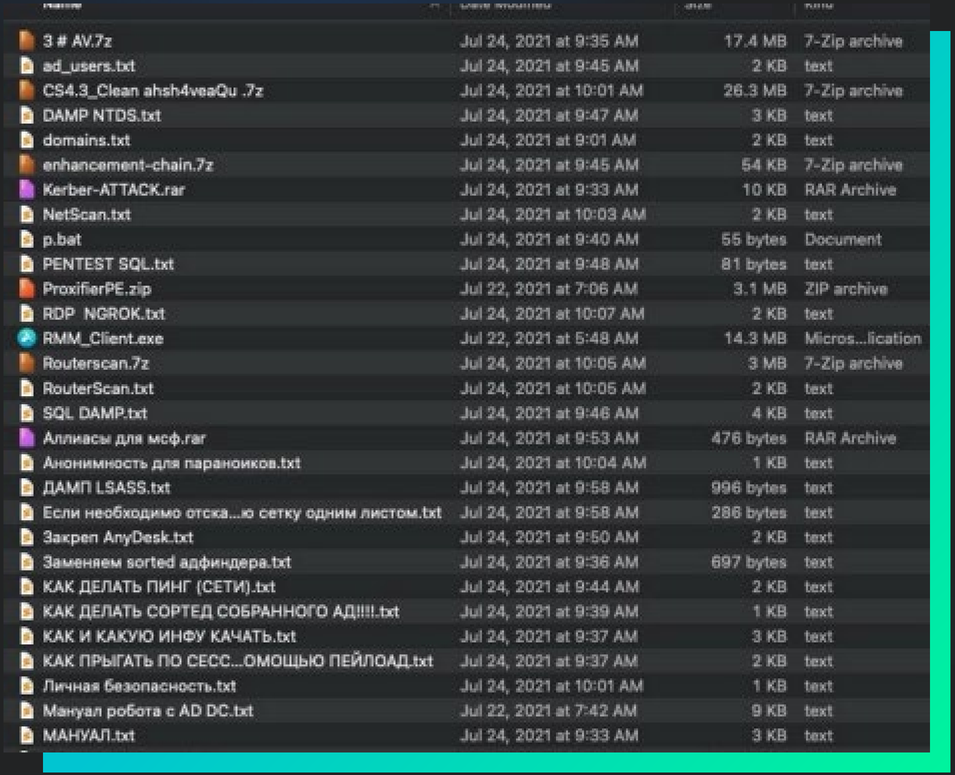
[redacted]
New User
MEMBER
27
ds 6
d Sep 2020
ation 0

October 21, 2020 at 05:12 AM This post was last modified: October 21, 2020 at 05:13 AM [redacted] Edited 1 time in total.

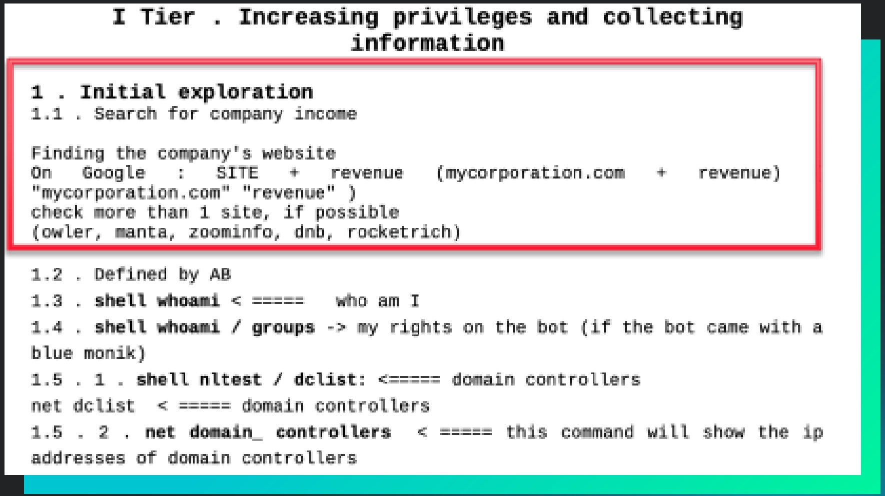
Following features :
✅ Small stub size
✅ Loader accept encryption Like botnets, Rats
✅ Bypass UAC
✅ Delete Shadow copy)
✅ Encryption speed faster than ever
✅ Uses a hybrid combination of encryption algorithms (AES-256 and RSA 2048)
✅ used asymmetric encryption It uses the public key in to encrypt the symmetric key
✅ Track the number of victims
Price $ 40
It is at an attractive price But it could rise in the future
Telegram:[redacted]
Email : [redacted]
Demo Videos : https://youtu.be/YaRLbncccBw

HUNTRESS

Cybercrime Employee Manuals



Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал робота с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text



I Tier . Increasing privileges and collecting information

1 . Initial exploration
1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue)
"mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

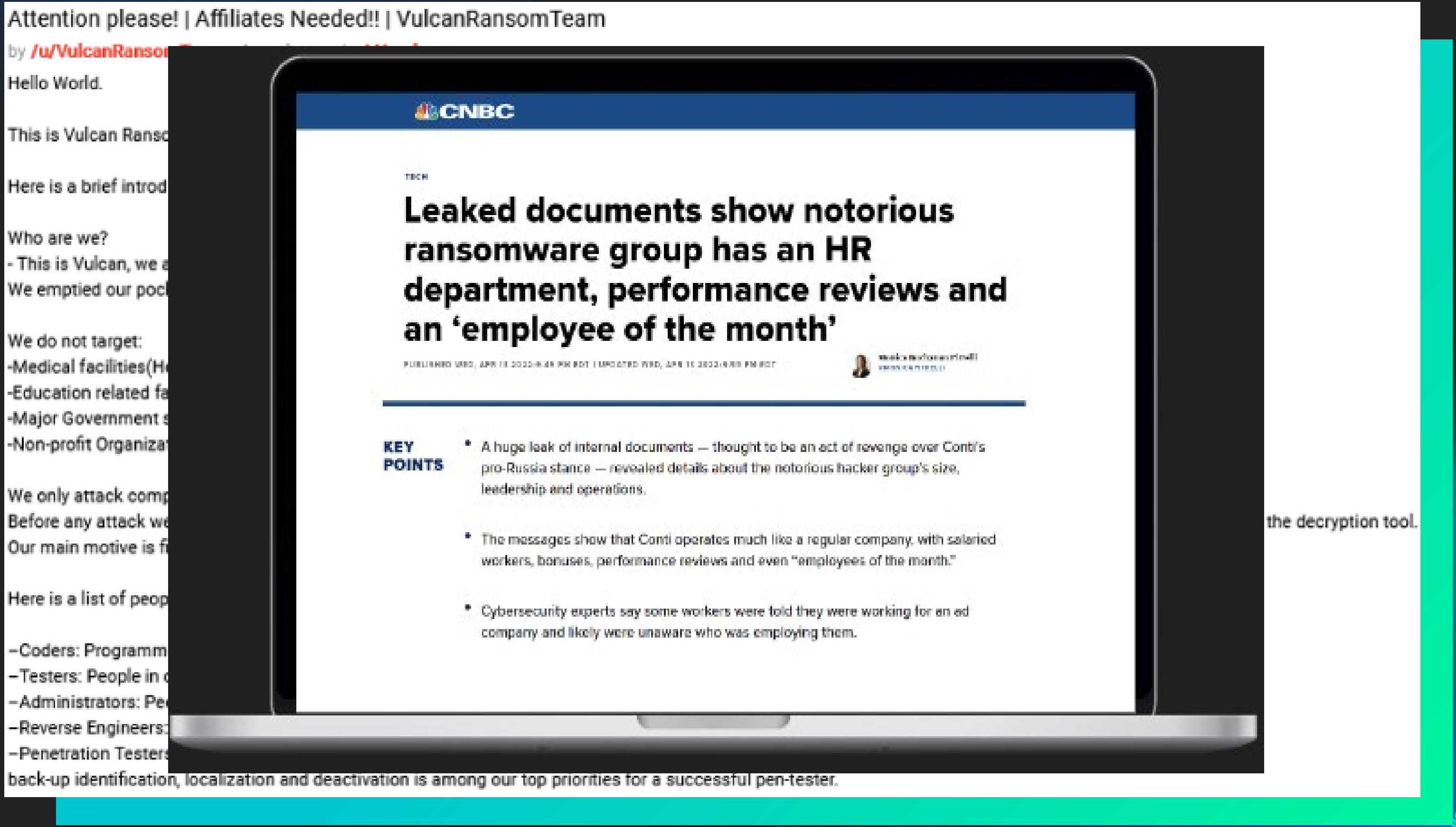
1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Hacker’s HR Team



Attention please! | Affiliates Needed!! | VulcanRansomTeam

by /u/VulcanRanso

Hello World.

This is Vulcan Ranso

Here is a brief introd

Who are we?
- This is Vulcan, we
We emptied our poc

We do not target:
-Medical facilities(H
-Education related f
-Major Government
-Non-profit Organiza

We only attack comp
Before any attack w
Our main motive is f

the decryption tool.

Here is a list of peop

–Coders: Programm
–Testers: People in
–Administrators: Pe
–Reverse Engineers
–Penetration Testers
back-up identification, localization and deactivation is among our top priorities for a successful pen-tester.

CNBC

TECH

Leaked documents show notorious ransomware group has an HR department, performance reviews and an ‘employee of the month’

PUBLISHED WED, APR 13 2022[illegible] PM EDT | UPDATED WED, APR 13 2022[illegible] PM EDT

[illegible]

KEY POINTS

- A huge leak of internal documents — thought to be an act of revenge over Conti’s pro-Russia stance — revealed details about the notorious hacker group’s size, leadership and operations.
- The messages show that Conti operates much like a regular company, with salaried workers, bonuses, performance reviews and even “employees of the month.”
- Cybersecurity experts say some workers were told they were working for an ad company and likely were unaware who was employing them.

Defense is Challenging!! What Can You Do?

Partner with an expert
Implement a comprehensive security solution
Harvest the low hanging fruit of cyber security

01 Asset Inventory

- Systems
- Applications
- Users

02 Basic IT Hygiene

- Patching
- MFA
- Least Privilege

03 Reduce Attack Surface

- SAT
- Remove Old Stuff

04 Plans

- BCP
- IRP

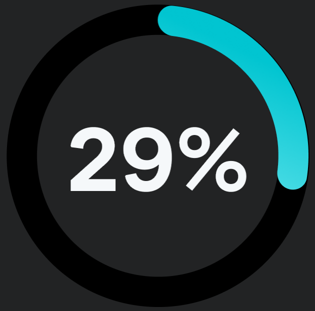
05 Operationalize

- Monitor
- Detect
- Respond

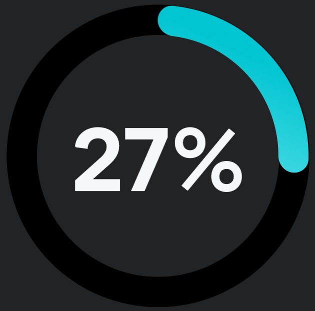
Why Monitor, Detect, Respond?

Attackers Are "Blending In"

To evade detection, threat actors are hiding within the noise of legitimate network operations and using living-off-the-land tactics in their intrusions.



of Huntress-identified incidents in Q3 2023 featured LOLBin or similar abuse as a tool for intrusion



of Huntress-identified incidents leveraged built-in scripting frameworks as a tool for intrusion

Source: *Huntress SMB Threat Report, Q3 2023*

HUNTRESS

Huntress Managed EDR

Malicious Process Behavior

Behavioral analysis to identify suspicious activity such as privilege escalation and lateral movement

Persistent Footholds

Identify abuse of legitimate applications and processes attackers use to hide in your environment

Ransomware Canaries

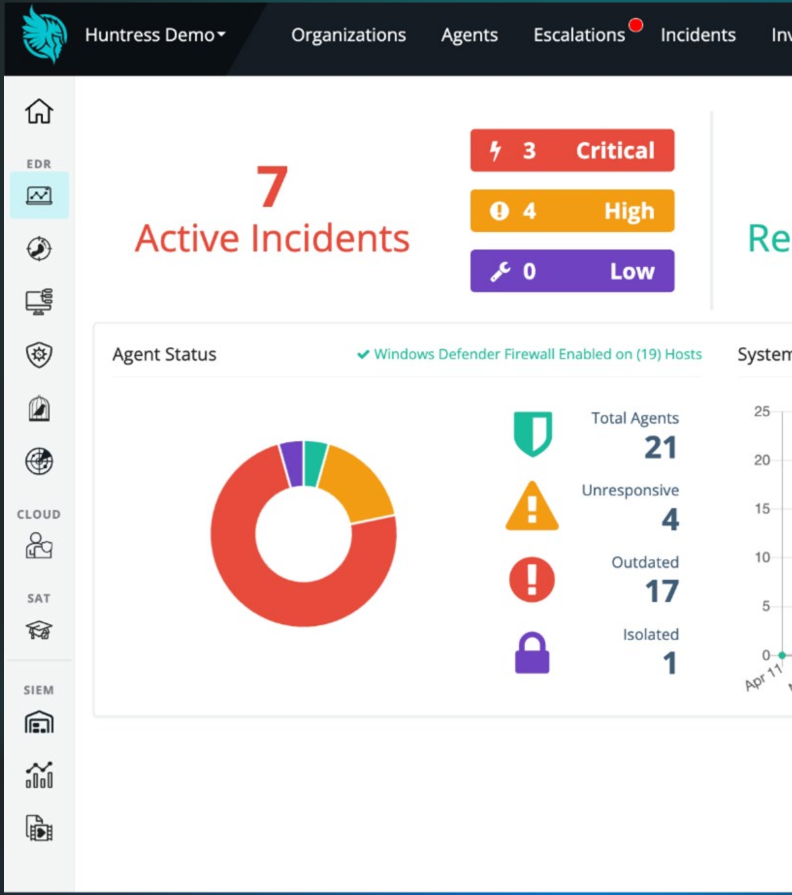
Small lightweight files monitored for early indications of ransomware

Open Port Detection

Reduce the attack surface by highlighting exposed entry points

Credential Reports

Detection of files believed to contain stored plaintext passwords



7 Active Incidents

3 Critical

4 High

0 Low

Agent Status

✓ Windows Defender Firewall Enabled on (19) Hosts

Total Agents 21

Unresponsive 4

Outdated 17

Isolated 1

Huntress complements your AV

Replace your AV with Microsoft Defender

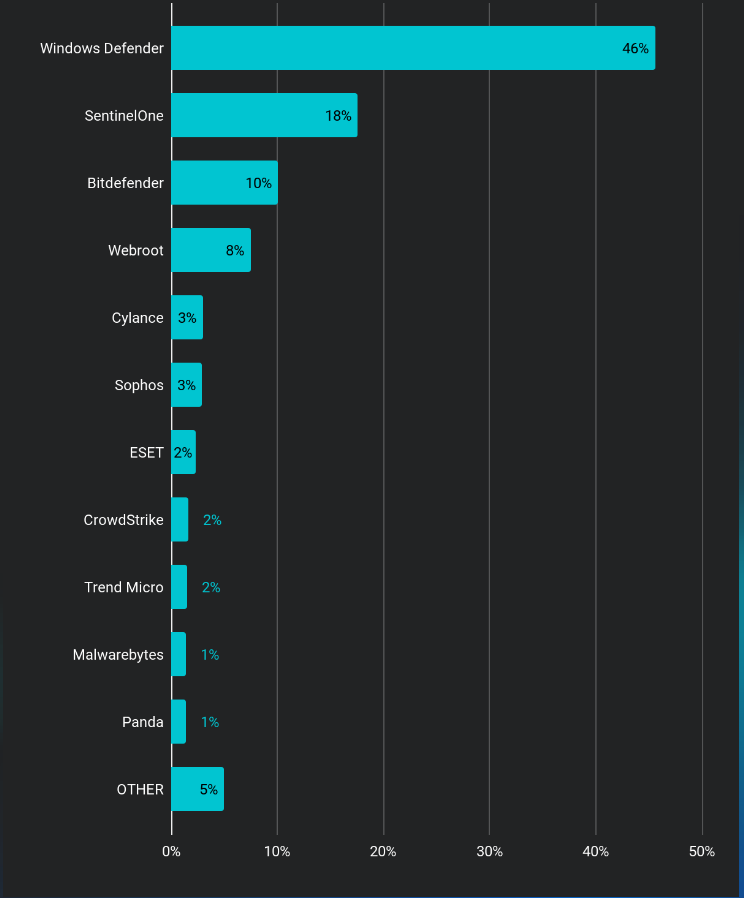
Huntress can manage free Microsoft Defender

Huntress can leverage native alerts from Microsoft Defender for Endpoint (MDE)

Run Huntress side-by-side with any AV

>50% of Huntress managed endpoints also utilize a non-Defender AV

Huntress consistently detects threats missed by 3rd party AV tools

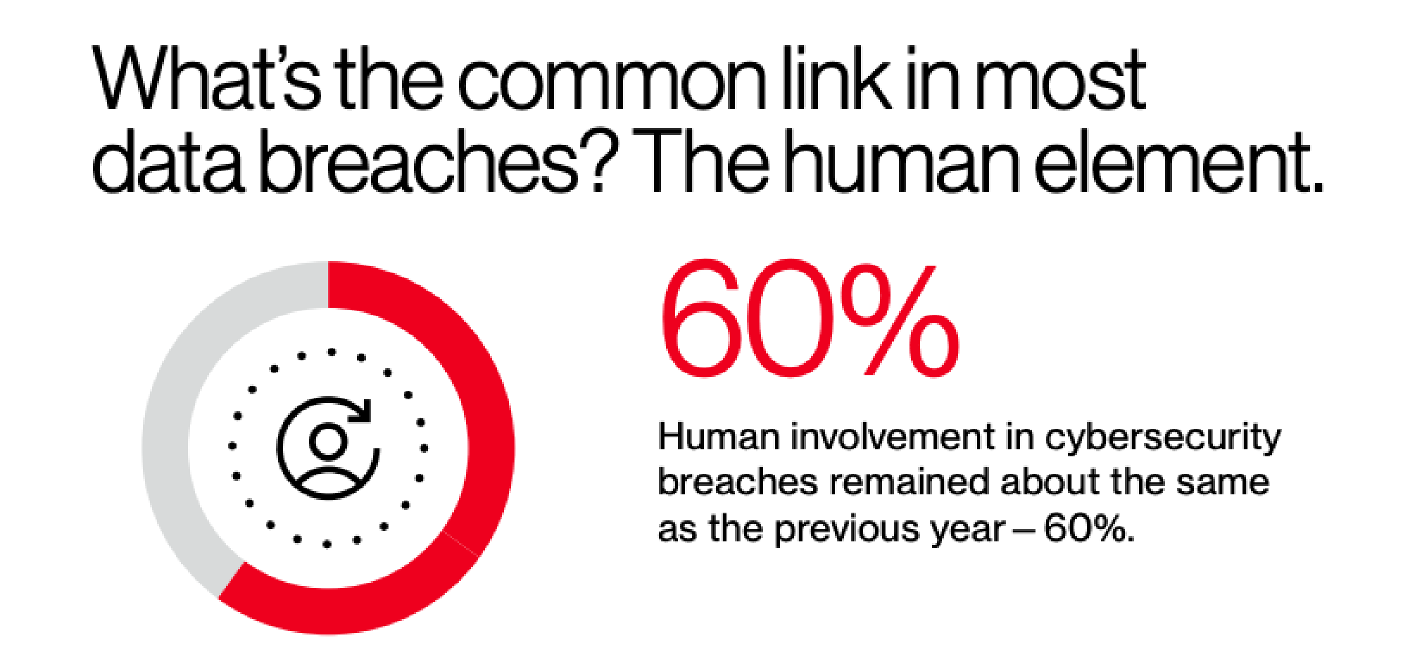


HUNTRESS

Humans

The largest attack surface of any organization

2025 Verizon DBIR



What's the common link in most data breaches? The human element.

60%

Human involvement in cybersecurity breaches remained about the same as the previous year – 60%.

Business Email Compromise (BEC)

01 Invoice Manipulation

02 Fraudulent Direct Deposit

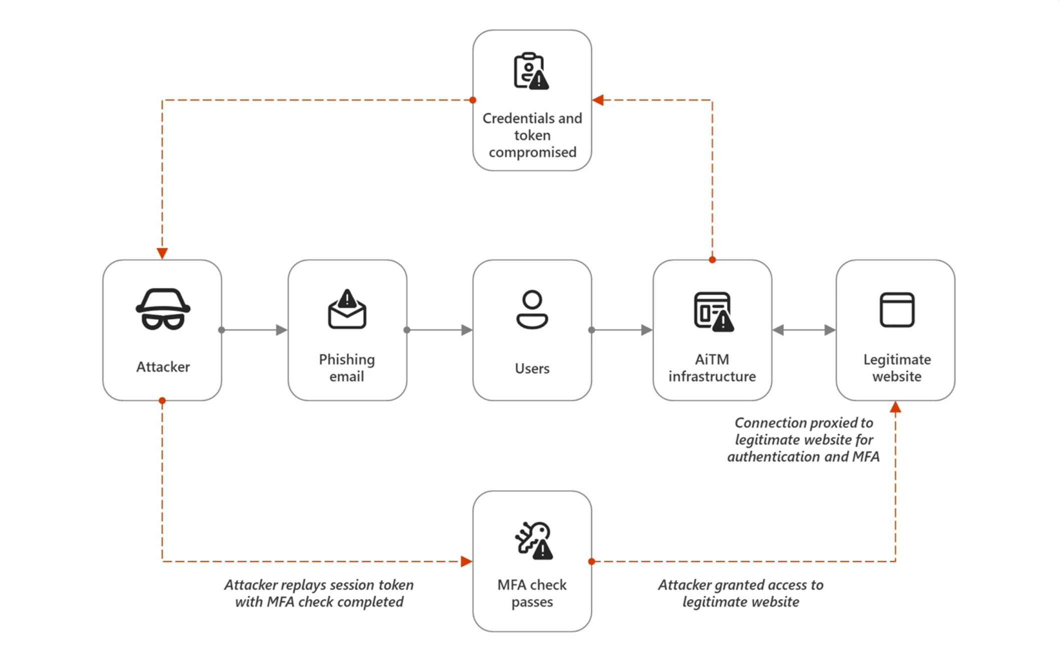
03 Fraudulent Wire Transfer

04 Pivot to other victims

05 Lateral Movement & Data Exfiltration

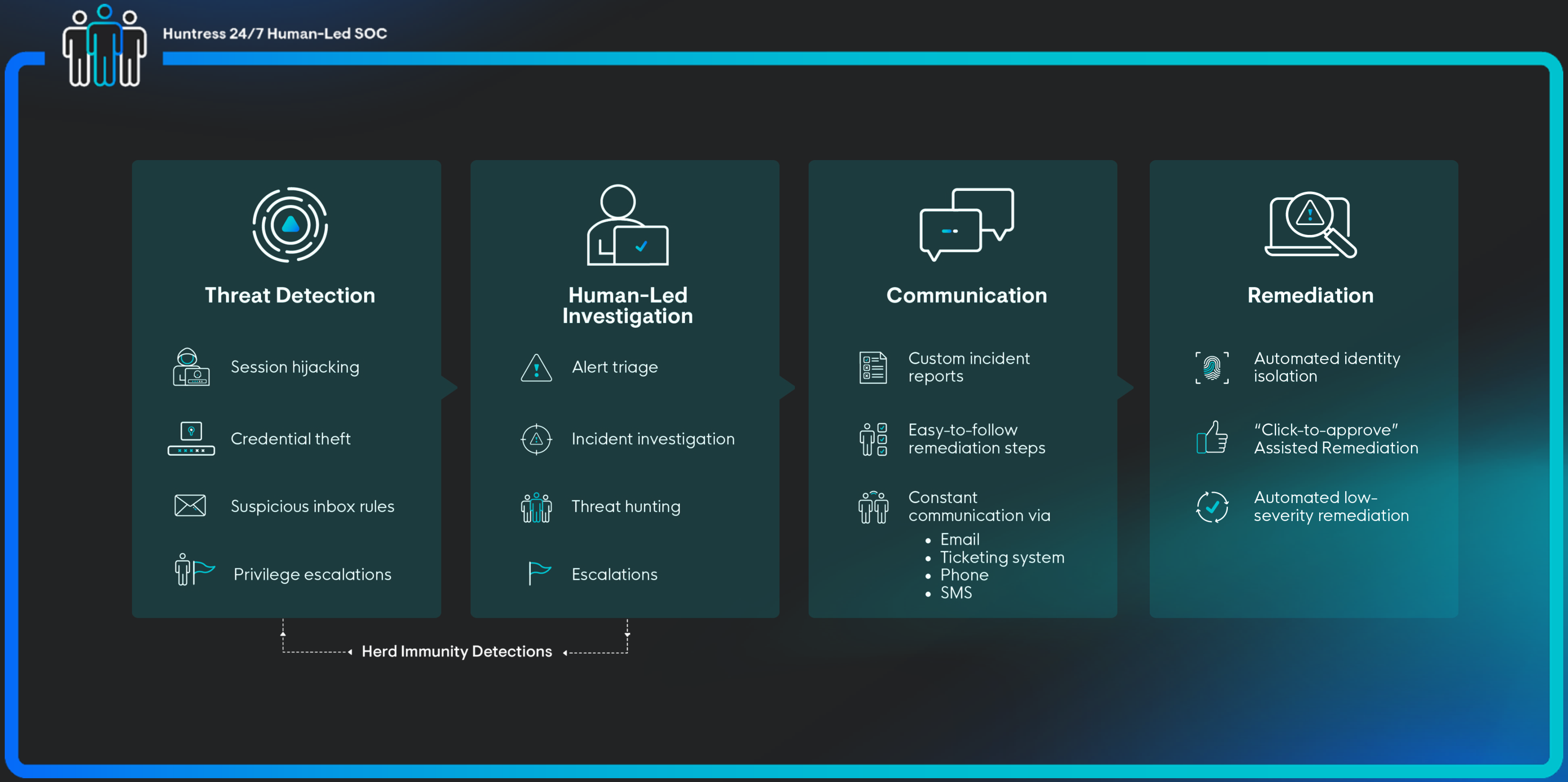
HUNTRESS

Surely, if my org uses MFA then I don’t need to be worried about identity attacks, right?


Credentials and token compromised
Attacker
Phishing email
Users
AiTM infrastructure
Legitimate website
Connection proxied to legitimate website for authentication and MFA
Attacker replays session token with MFA check completed
MFA check passes
Attacker granted access to legitimate website

Example of token theft via an Adversary in the Middle (AiTM)

Identity Threat Detection & Response (ITDR)



Huntress 24/7 Human-Led SOC

Threat Detection

- Session hijacking
- Credential theft
- Suspicious inbox rules
- Privilege escalations

Human-Led Investigation

- Alert triage
- Incident investigation
- Threat hunting
- Escalations

Communication

- Custom incident reports
- Easy-to-follow remediation steps
- Constant communication via
  - Email
  - Ticketing system
  - Phone
  - SMS

Remediation

- Automated identity isolation
- "Click-to-approve" Assisted Remediation
- Automated low-severity remediation

Herd Immunity Detections

What about monitoring beyond EDR and ITDR…

Throw the Kitchen Sink At It?

Orgs started adopting tools at exponential rates…

Tools In Use	Percentage of Orgs
<10	14%
10-25	39%
26-50	26%
51-75	17%
>75	36%

More tools, more problems…

- **89%** of organizations report a **shortage of skills** and personnel
- **63%** report operational workflows are **too complex** or disorganized to be effective
- **51%** of users want to **reduce the number of tools** used as part of SOC workflows
- **49%** of users want to implement a **common interface** or work surface for all SOC workflow activities

HUNTRESS

SIEM Goals

Built to collect, designed to detect

Log Centralization

Collection of disparate log sources

73% Say IT changes quarterly

64% Lack central visibility and collection

53 Average security tools in use

Threat Detection

Correlate data, find the exposures

#1 Reason for SIEM adoption for Mid/Ent.

66% Report silos affect efficacy

3 Hours to investigate one incident

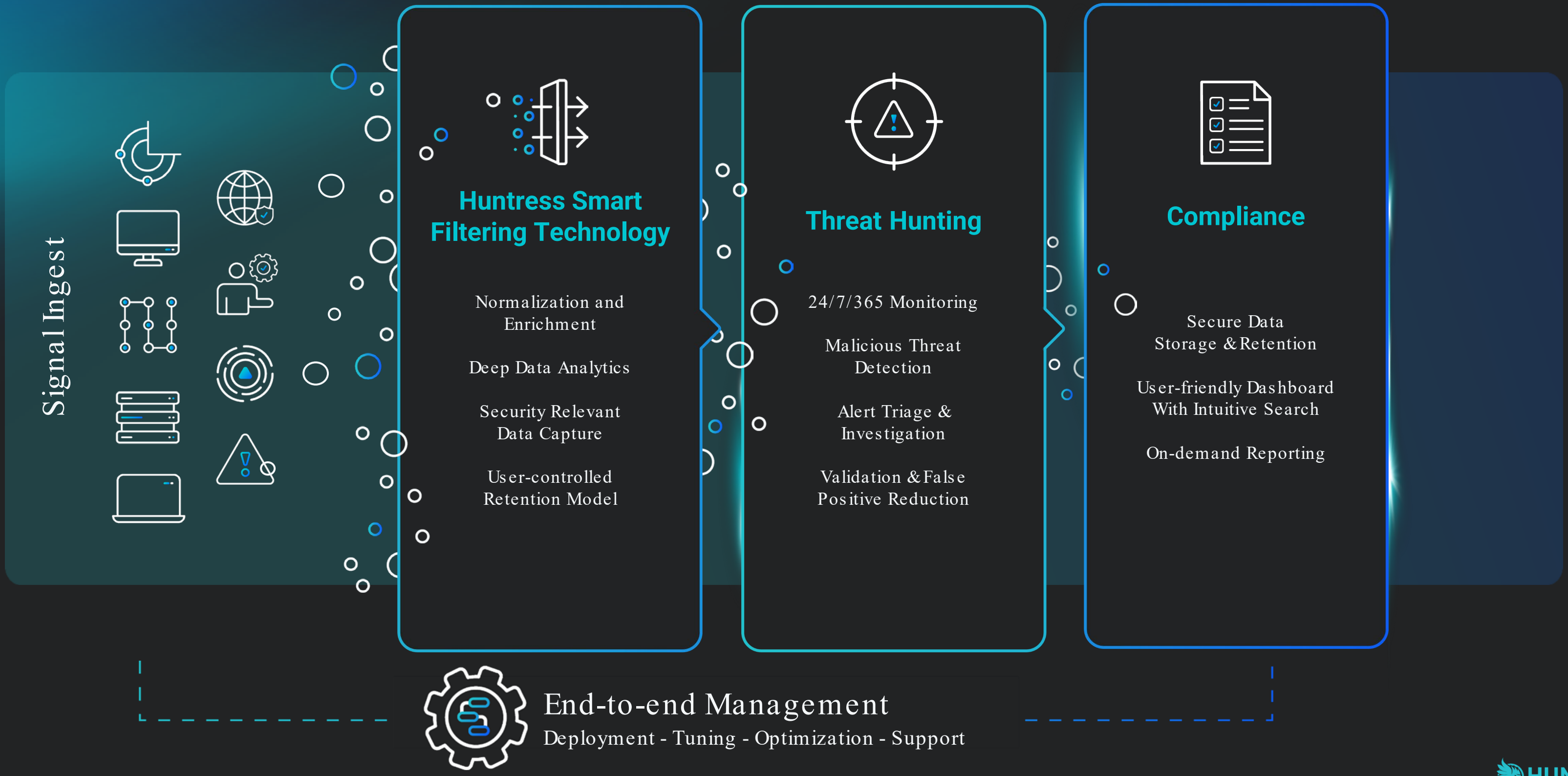
Reporting and Compliance

Map out requirements and areas of risk

53% Cannot keep up with compliance req’s

#1 Reason for SIEM adoption for SMB

Huntress Managed SIEM



Signal Ingest

Huntress Smart Filtering Technology

Normalization and Enrichment

Deep Data Analytics

Security Relevant Data Capture

User-controlled Retention Model

Threat Hunting

24/7/365 Monitoring

Malicious Threat Detection

Alert Triage & Investigation

Validation & False Positive Reduction

Compliance

Secure Data Storage & Retention

User-friendly Dashboard With Intuitive Search

On-demand Reporting

End-to-end Management

Deployment - Tuning - Optimization - Support

HUNTRESS

Need Employee engagement for successful Cyber Security

Poorly trained users are human vulnerabilities hackers will exploit

You can’t patch humans… but you can teach them

Robust training programs turn learners into your first line of defense

Managed SAT

Security Awareness Training that’s fun and effective for the 99%.

Our Security Awareness Training enables better security outcomes by using story-based learning to empower end users with the knowledge to protect themselves and the company.

- Huntress SAT features episodic content engages end users by doing away with fear and immersing them in the adventures of 5 yr old hacker prodigy DeeDee.
- SAT come loaded with easy-to-use features including simulated phishing, gamified training, and detailed reporting.
- Huntress SAT enables better security outcomes by providing a large library of story-based content that prepares learners for real-world threats.
- Powerful automated reporting makes compliance audits easy while providing executive, group and user level insights.

Questions?