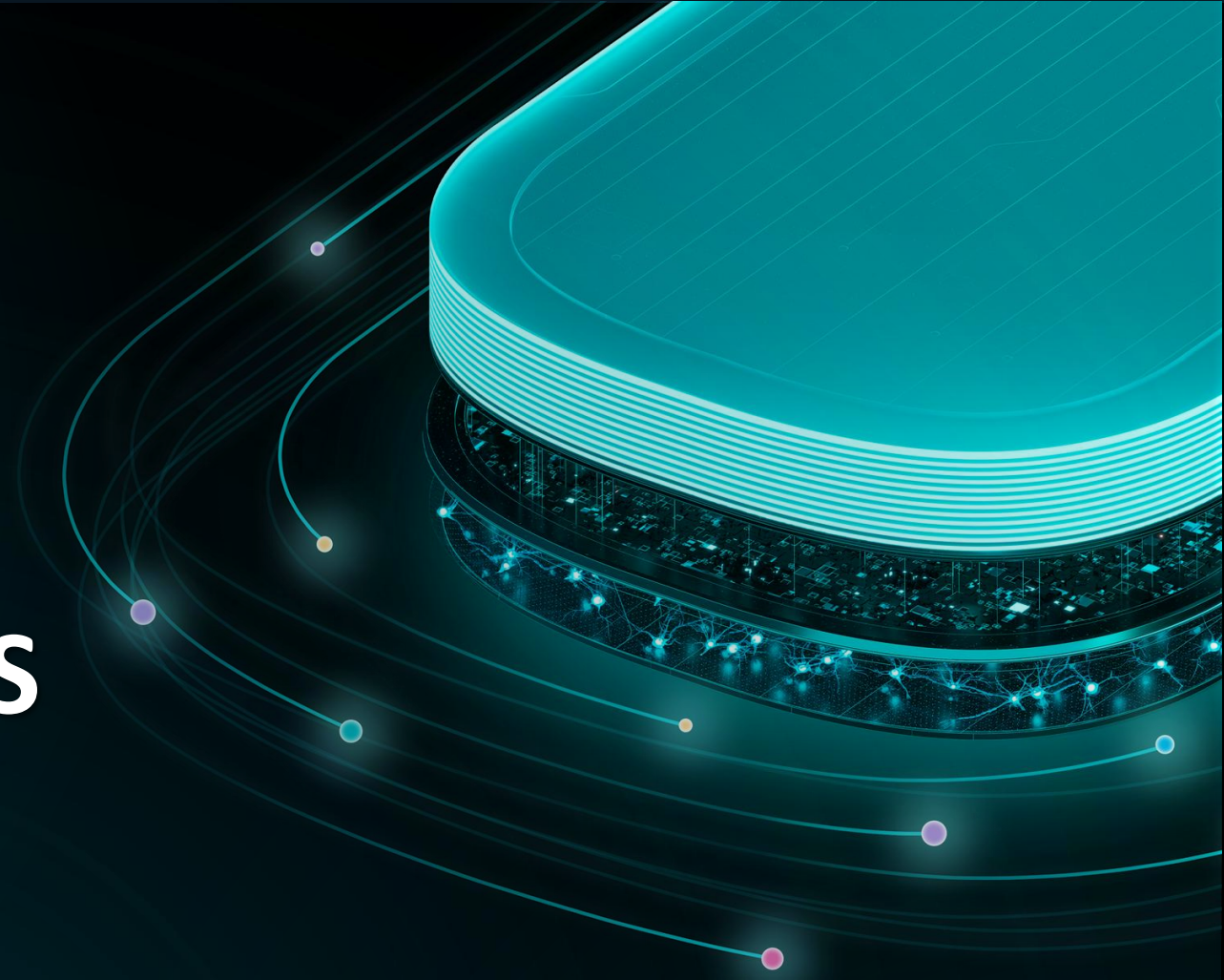


Cybersecurity

Progress. Protected.



ANATOMY OF THREDS

Behind the curtain of cybercrime

VÁCLAV ZUBR
Solution Architect

Cybersecurity
Progress. Protected.

Hundreds of analyzed hands-on-keyboard attacks

ESET | Data, Systems, Specialists



Identification



Analysis



Monitoring



Know-how

ESET | Police Operations Support

Significant support for law enforcement authorities in tackling the most serious threats, including catching malware creators and criminals

- Operation Amadey & Stealc Endgame (2026) – disruption of the Amadey botnet and Stealc infostealer
- Operation Danabot Endgame (2025) – Danabot infostealer infrastructure breach
- Operation Lumma Stealer Disruption (2025) – Crackdown on the Lumma MaaS infostealer
- Operation Magnus (2024) – neutralization of RedLine and META infostealers
- Operation Grandoreiro (2024) – neutralization of the Grandoreiro banking malware
- Operation First Light (2024) – apprehending perpetrators of global phishing scams
- Next: Action against Gamarue/Andromeda botnet, Emotet malware, Zloader botnet...

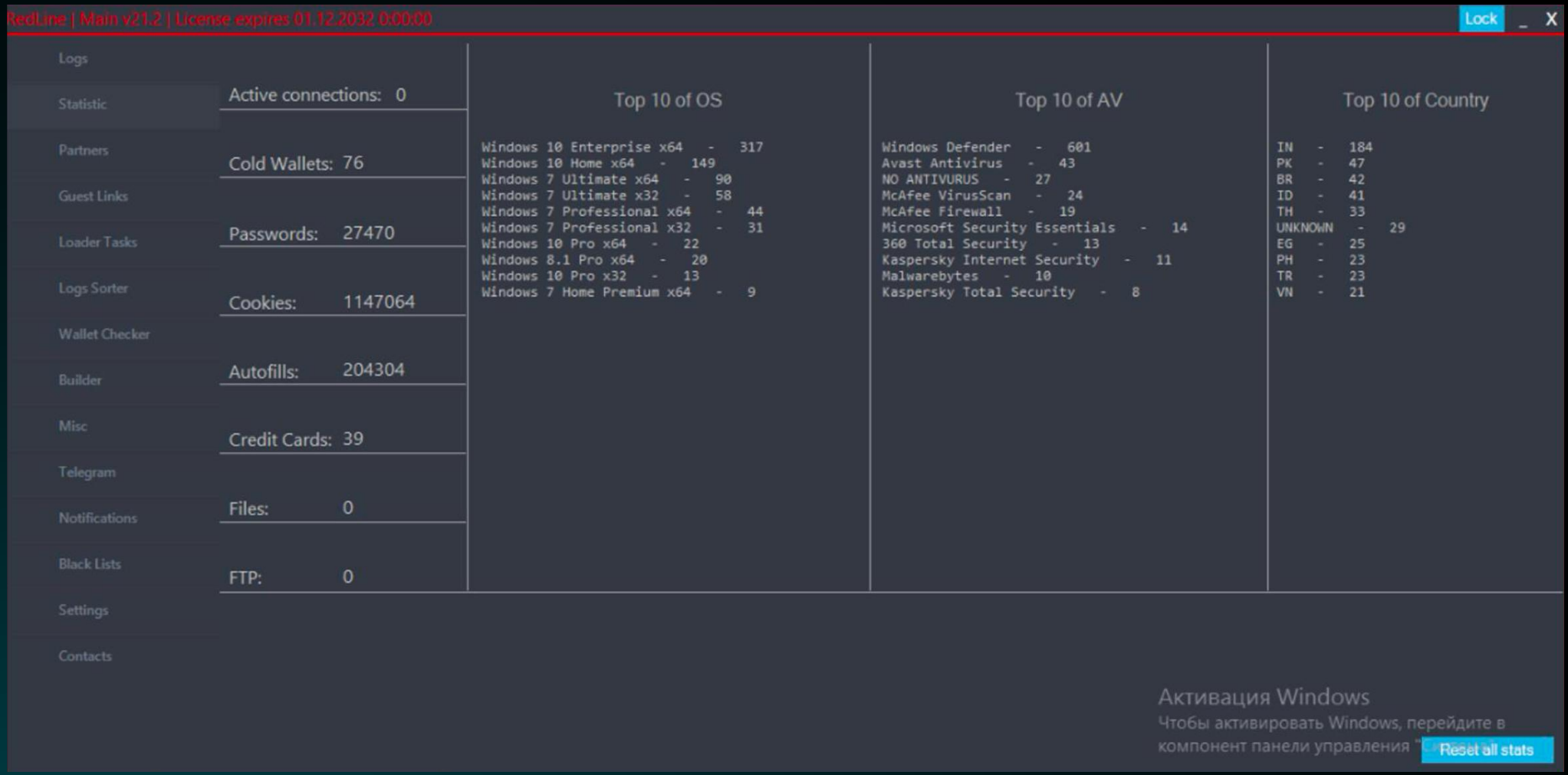
Infostealers

Infostealer as a Service | Initialization

Telemetry data is sent after the initial run

- Username
- Exact OS version
- Geolocation
- Public IP address
- Operated security software
- Hardware Specifications of the Device
- And more

Infostealer as a Service | Initialization



Infostealer as a Service | Theft

Data is stolen primarily from WEB BROWSERS

- Saved credentials in browsers
- Browser cookies, including authentication and session tokens
- Complete browser history
- Credentials from installed apps
- Browser extension data

- **Business environment: access to VPNs, web portals, cloud services, and email accounts**

Infostealer as a Service | Theft

Extensions Chrome

Coinbase Wallet, Nifty Wallet, Trust Wallet, BitClip, Binance Chain Wallet, Coin98 Wallet, Liquality Wallet, HAVAH Wallet, Aegis Authenticator, CommonKey, BitPay, Math Wallet, Rainbow, ZilPay, MetaMask, Fewcha Move Wallet, Bitbox, Solana Wallet, Authy, Digital Bitbox, Frontier Wallet, BrowserPass, Sollet, Opera Wallet, iWallet, Phantom, SubWallet - Polkadot Wallet, KeePass, Keeper Password Manager, KeepKey, LastPass Authenticator, xverse.app, Leap Cosmos Wallet, EQUAL Wallet, Coinhub, Klever Wallet, Elli-Sui Wallet, Waves Keeper, MetaWallet, Avira Password Manager, Yoroi, Rabet, Petra Aptos Wallet, Morphis Wallet, TezBox, XDCPay, Fluvi Wallet, FreeOTP, Zoho Vault, ICONex, OneKey, Dashlane, Atomic Wallet, Duo Mobile, Trezor Password Manager, NeoLine, Byone, MOBOX WALLET, Blade-Hedera Web3 Digital Wallet, Venom Wallet, Braavos Smart Wallet, BitKeep, BRD, Bitwarden, Splikity, Edge, SAASPASS, KeePassXC, Jaxx Liberty, Ledger Live, XDEFI Wallet, Keeper, Norton Password Manager, compass-wallet-for-sei, zkPass TransGate, Telos Authenticator, BitApp Wallet, Hashpack, Terra Station, Authenticator, LastPass, Guarda, KHC, GreenAddress, Cyano Wallet, OTP Auth, NordPass, RoboForm, GAuth Authenticator, Bread, Swash, Electrum, Pontem Aptos Wallet, Rise - Aptos Wallet, Ledger Wallet, Coinomi, Keplr, DualSafe Password Manager, Mycelium, 1Password-fox, MultiPassword, MultiversX DeFi Wallet, Ronin Wallet, Samourai Wallet, SafePal, MYKI, EOS Authenticator, Glass wallet-Sui wallet, Exodus, Finnie, TronLink, MEW CX, Wombat

Extensions Edge

KeePassXC, MYKI, Binance Chain Wallet, MetaMask, Rainbow, Terra Station, Keeper Password Manager, Ronin Wallet, Keplr, SafePal, Dashlane, Trust Wallet, 1Password, Math Wallet, LastPass, RoboForm, Wombat, Braavos Smart Wallet, TezBox, Authenticator, bitwarden, EQUAL Wallet, Waves Keeper, Exodus Web3, Yoroi

Extensions Opera

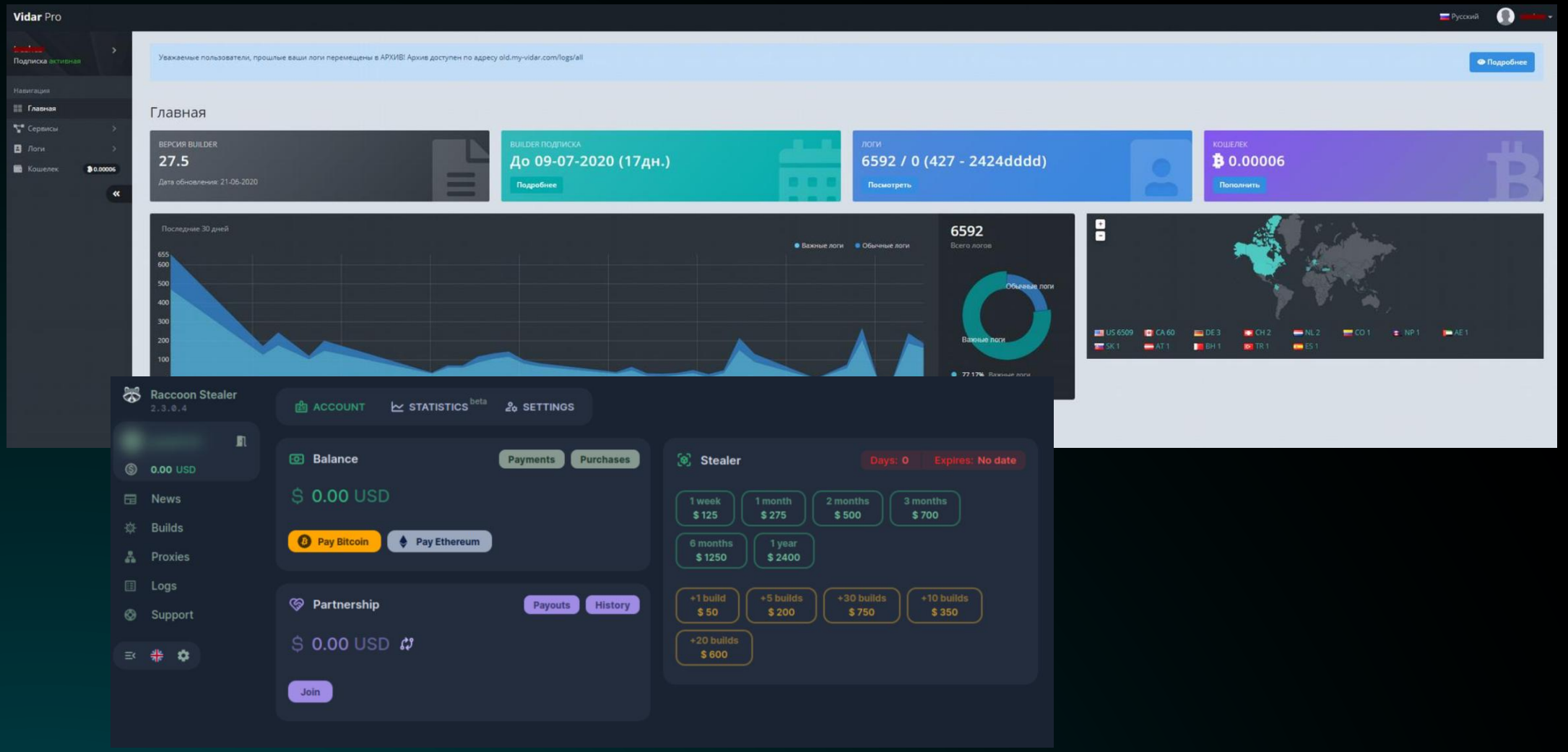
MetaMask, Guarda Wallet, BitKeep, Waves Keeper

Infostealer as a Service | Other Features

Some infostealers have advanced extension features

- Keystroke capture
- Swapping account numbers and crypto addresses in the clipboard
- Capturing copied information (Ctrl+C)
- File search and exfiltration
- Ability to execute additional malicious code
- Remote command execution (e.g. reverse shell)

Infostealer as a Service | Control Panels



Infostealer as a Service

Professionalization of cybercriminals



IaaS operators

They develop infostealers and operate their control infrastructure



Initial access providers

They acquire and sell access to compromised organizations



Intersection operators

They use the acquired accesses to further penetrate the network

Infostealer as a Service

Professionalization of cybercriminals



IaaS operators

They develop infostealers and operate their control infrastructure



LaaS Operators

They operate malware delivery and execution services



Initial access providers

They acquire and sell access to compromised organizations



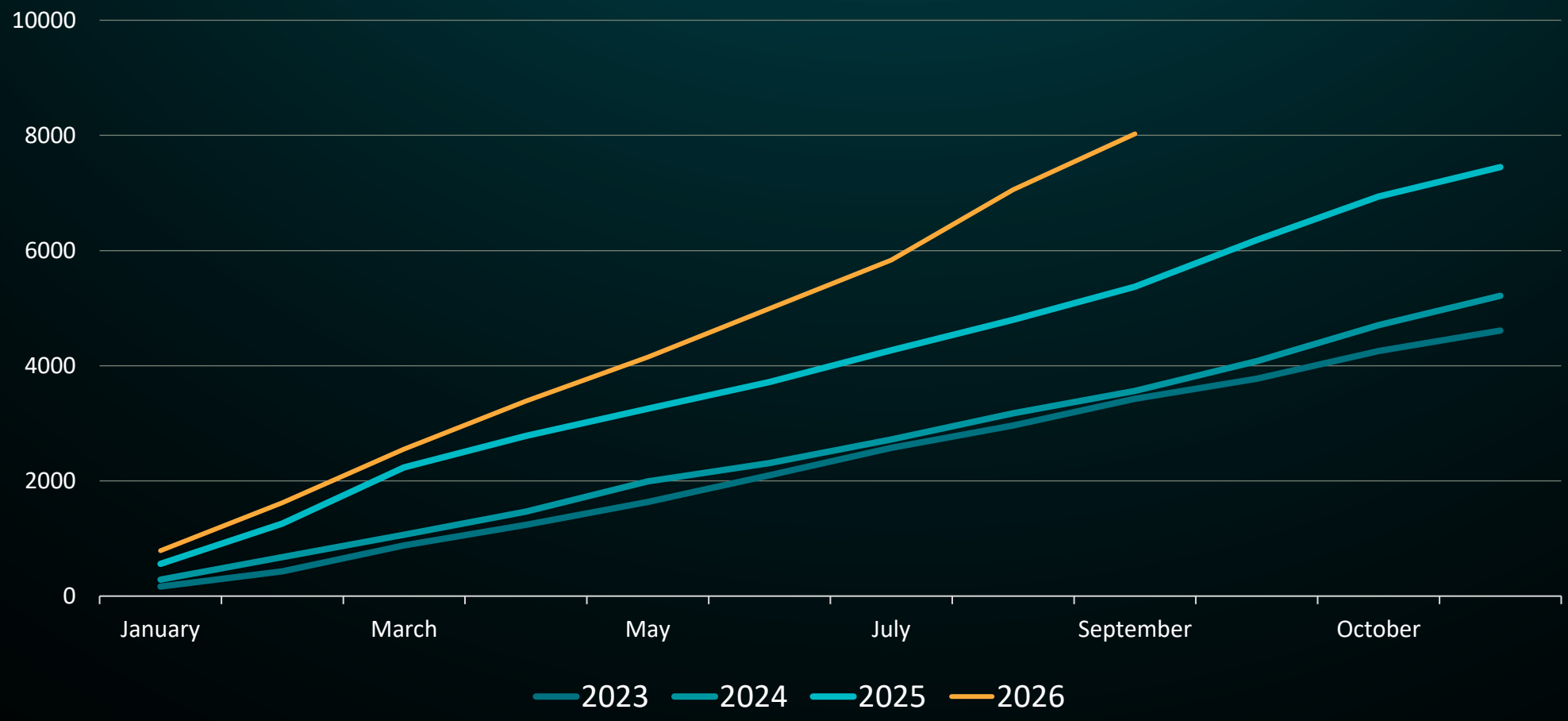
Intersection operators

They use the acquired accesses to further penetrate the network

Ransomware



Ransomware victims published on Data Leak Sites



Ransomware as a Service

Professionalization of cybercriminals



RaaS operators

They develop ransomware and run the associated infrastructure



Intersection operators

They penetrate networks, gain control over them, deploy ransomware



Initial access providers

They acquire and sell access to compromised organizations

Crackdown on RaaS gangs

BlackCat (2023) savings 68mil. USD

- Russian-speaking group active since 2021
- Multiplatform ransomware (Windows & Linux)
- Double blackmail, "Big Game Hunting"
- Dozens of servers secured by police operation

LockBit (2024) savings 120+mil. USD

- Russian-speaking group active since 2019
- Up to ~25% of all ransomware attacks across sectors
- Some developers arrested, available servers seized
- Gigabytes of internal data published

Crackdown on RaaS gangs

Phobos (2025)

- The target of the 8Base group using the Phobos ransomware
- Detaining 4 people from the 8Base management, 27 servers shut down
- Cooperation between authorities from 14 countries

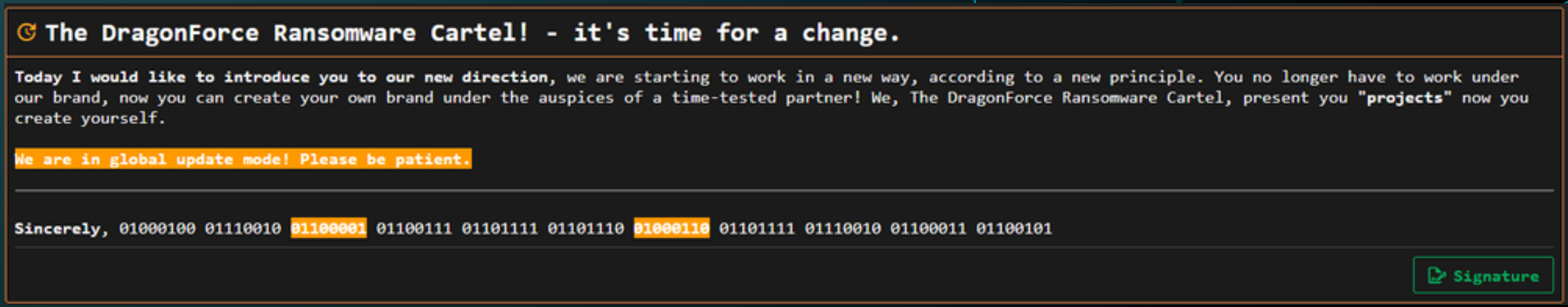
KillSec (2026)

- RaaS KillSec Development Group
- Taking control of 5 key servers
- Arrest of three suspects

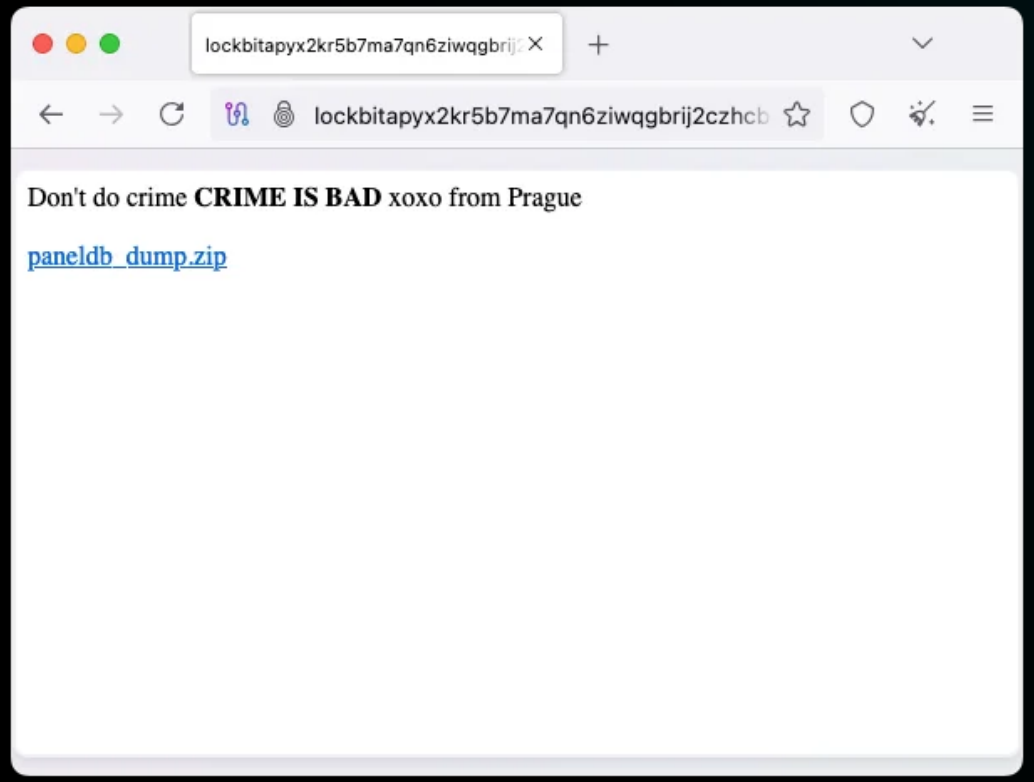
Gangs attacking each other

RansomHub - Hostile takeover by DragonForce

- Dominant Russian-speaking RaaS group
- Ransom directly to cybercriminals
- Only 10% for RaaS RansomHub
- Technically advanced, custom EDR Killers



Hack Hackers | LockBit & Everest







Present
Time Manually
attacks carried out

Modern blackmail attacks



Get the first approach



System, Users, Network Analysis



Download malware, utilities, and scripts



Obtaining legitimate credentials



Lateral movement in the network



Exfiltration of sensitive data



Retirement of backups and data encryption



Ransom Payment Request

Different groups, same procedures

ESET observes similar tactics, techniques, and practices across different groups of attackers

- Qilin, Play, Medusa, BianLian, Clop
- Conti, REvil, RansomHub, BlackCat, LockBit
- Including dozens of monitored APT groups



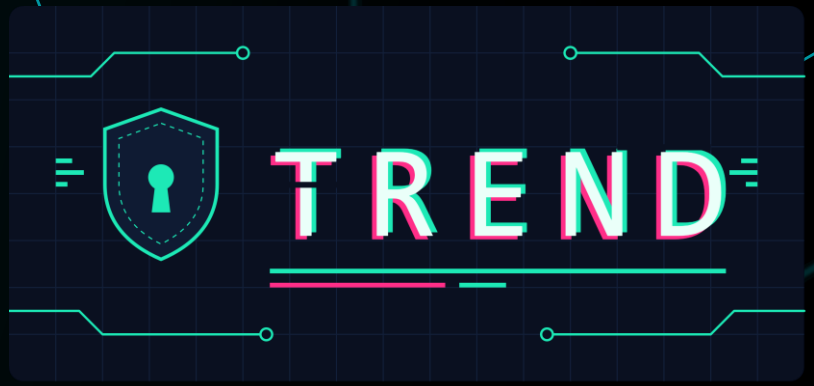
12 TOP groups, ~90 overall

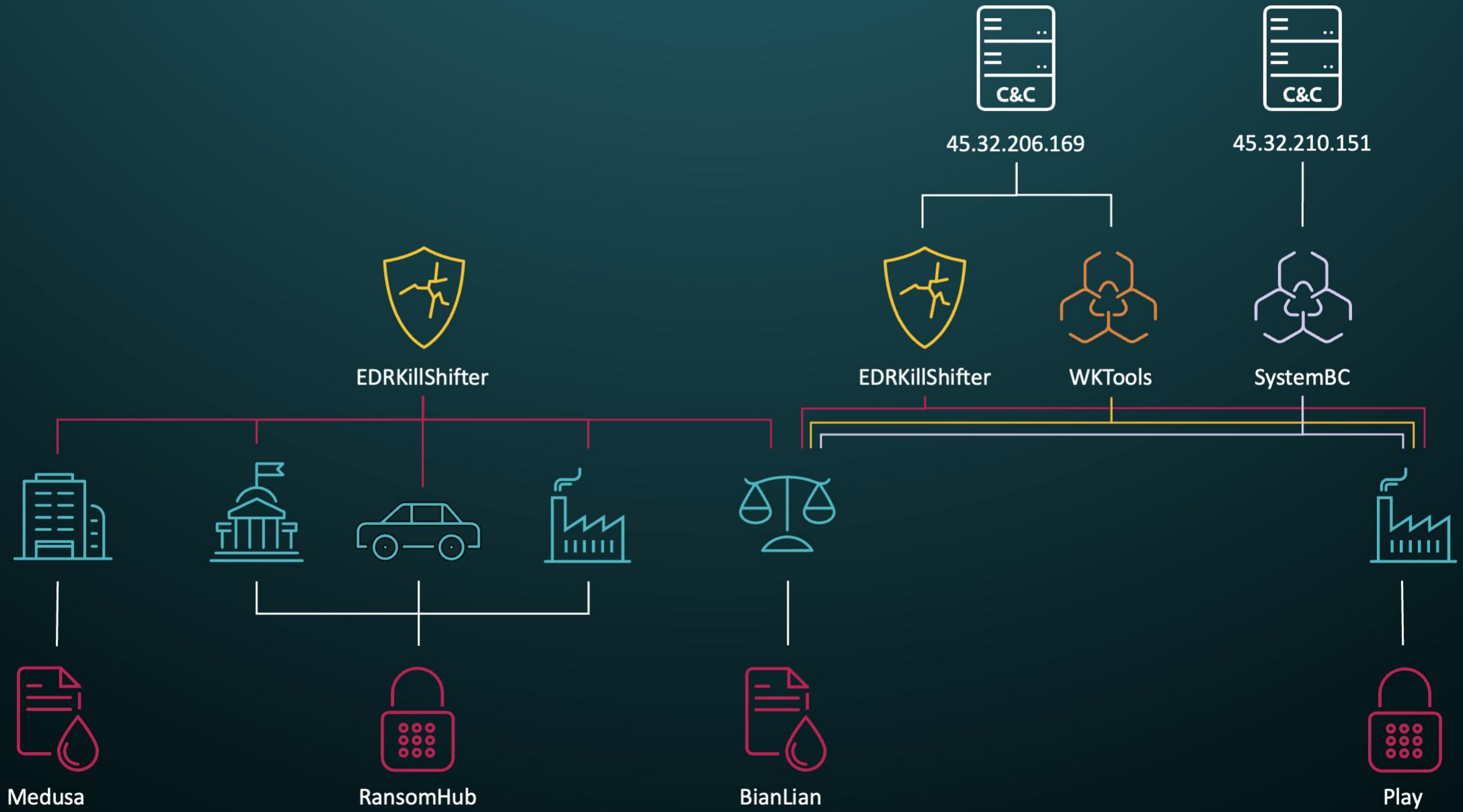
Up to hundreds of actors using malware of major RaaS groups

EDR Killers | BYOVD

An attacker installs a legitimate but vulnerable driver on the system to gain unauthorized access to the operating system's kernel functions; this is then **misused to compromise or disable security software**

- Scripts, (anti-)rootkits, vulnerable drivers, OS weaknesses
- The first cases of abuse by APT groups (Slingshot)
- Today we observe ~4 new EDR Killers per month
- The goal is primarily MS and "native next-gens" solutions
- Exploiting existing vulnerable drivers as well




C&C
C&C
45.32.206.169
45.32.210.151
EDRKillShifter
EDRKillShifter
WKTools
SystemBC
Medusa
RansomHub
BianLian
Play



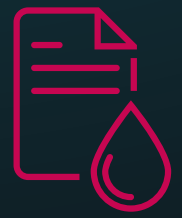
EDRKillShifter



Jellyfish



RansomHub



BianLian



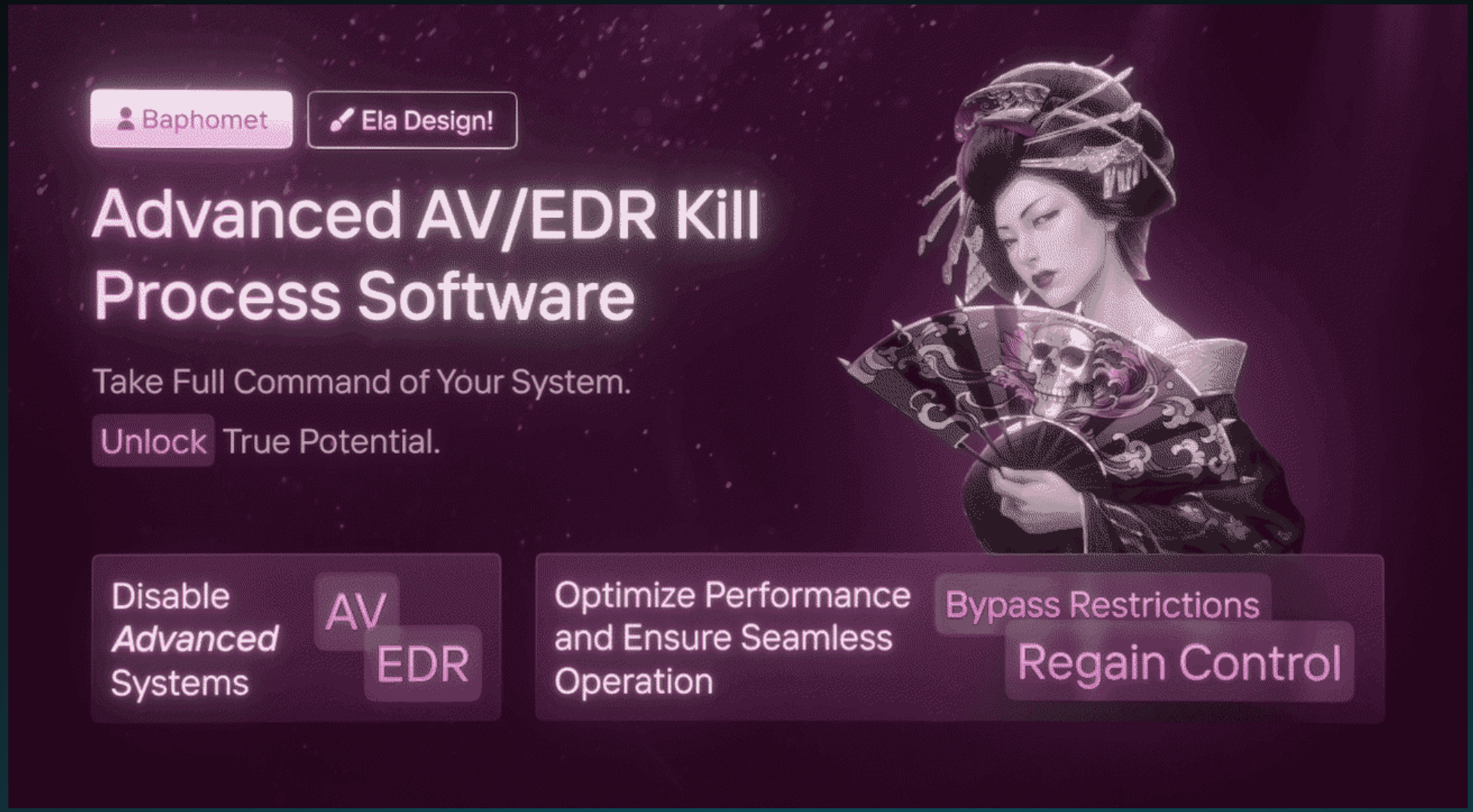
Game

EDR Killer | probably created with the help of AI

```
  print("[*] %s\n", "Try common device names...");
idx2 = 0;
if ( devices_list[0] )
{
  idx = 0;
  deviceName = devices_list;
  while ( 1 )
  {
    if ( v6 )
    {
      deviceName = &devices_list[idx];
      print("    Try: %ls\n", *deviceName);
    }
    FileW = CreateFileW(*deviceName, 0xC0000000, 0, 0, 3u, 0x80u, 0);
    if ( FileW != -1 )
      break;
    ++idx;
    ++idx2;
    deviceName = &devices_list[idx];
    if ( !*deviceName )
    {
      v5 = v36;
      goto LABEL_59;
    }
  }
```

```
  if ( v6 )
  {
    print("[+] %s\n", "Find the device");
    print("    device name: %ls\n", devices_list[idx2]);
  }
}
else
{
  FileW = -1;
  print("[-] %s\n", "Could not open device");
  if ( !v7 )
  {
    print("\n");
    print("Possible fixes:\n");
    print(" 1. Verify the device name is correct\n");
    print(" 2. Ensure the driver is properly loaded\n");
    print(" 3. Specify the correct device name using -d option\n");
    print(" 4. Run this program as Administrator\n");
  }
  if ( v5 )
    j__free_base(v5);
}
```

EDR Killer | as a service



EDR Killer | Silencer & Freeze

Silencer – interruption of communication

It exploits the legitimate Windows Filtering Platform (WFP) technology, which allows you to control and filter network communication. An attacker uses WFP to create network filters that block outbound communication between the security agent and its control infrastructure. At the same time, the security software continues to run and can detect threats locally, but cannot send security events to the central console.

Freeze – suspend processes

It abuses the legitimate Windows Error Reporting (WER) mechanism, which is used to diagnose application errors. When creating a memory dump, the system temporarily suspends the threads of the analyzed process. The attacker uses this mechanism to suspend the security process and then blocks the Windows component that was supposed to complete the diagnostics and reactivate the process. The security software thus remains running, but its process stops performing its activity.

Undetectable ransomware

~~Undetectable ransomware~~



UndetectableEDR Killer

ESET | EDR Assassins

Protection with ESET AV

- PUSA Vulnerable Driver Installation Detection (Win64/WnBios)
- Detection of the killer itself (Win64/HackTool)

Protection with ESET XDR

- Vulnerable Driver Storage Detection (Q1302)
- Detecting Driver Loading from Abnormal Location (D1303)
- Vulnerable Driver Load Detection (Q1301, D1302)
- Detecting the loading of a driver known for exploitation (Q1303)
- WFP Detection and WerFaultSecure Exploit (C0460...)

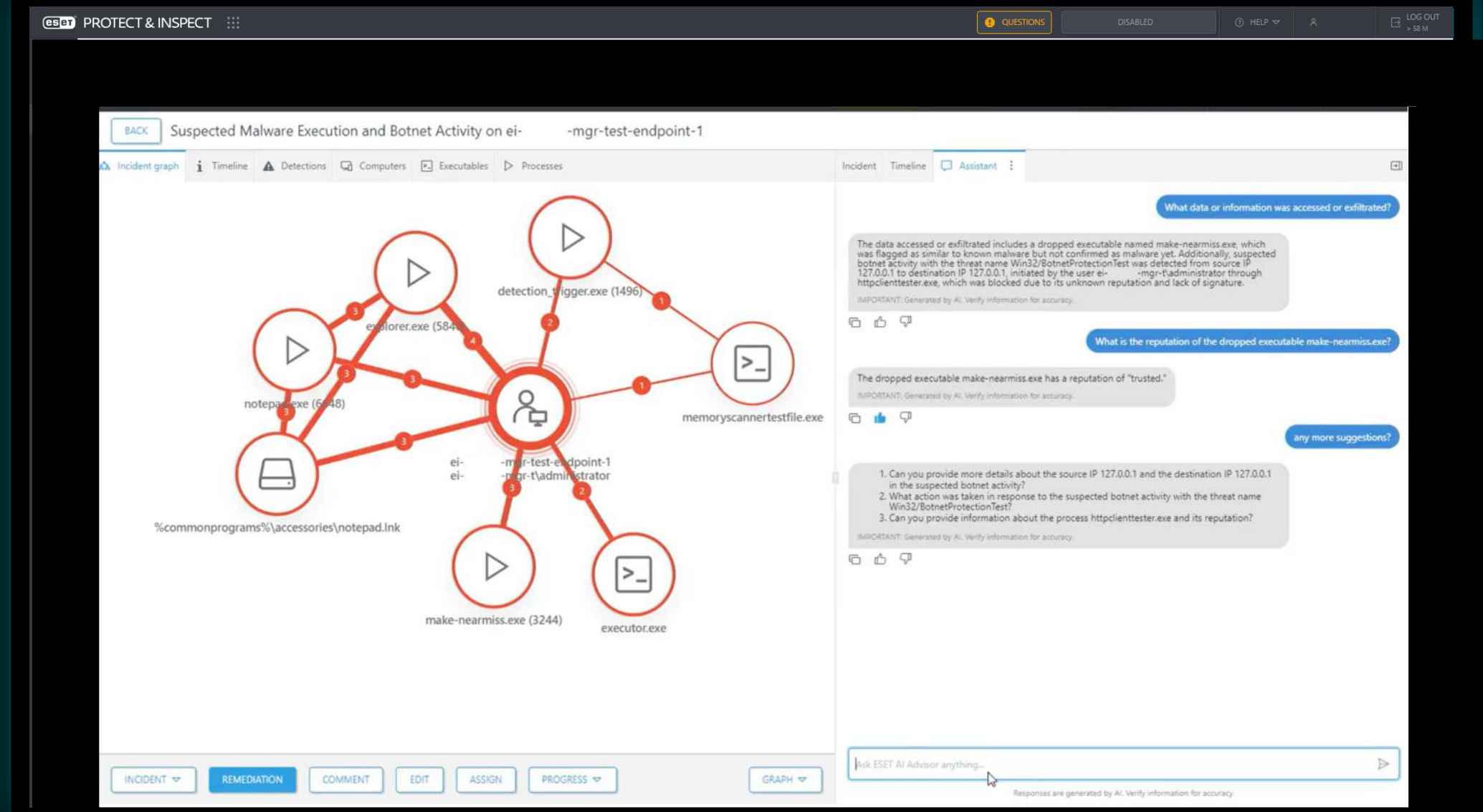


ESET | EDR Assassins

Protection with ESET PROTECT

- Attack vector mitigation (mail security, MFA, vulnerability scanner)
- Privilege escalation (patch management)
- Robust self-defense
- Incidents with Minimum False Positive (Remote Management)
- Security monitoring (MDR/SOCaaS services)




PROTECT & INSPECT
QUESTIONS
DISABLED
HELP
LOG OUT
BACK
Suspected Malware Execution and Botnet Activity on ei- -mgr-test-endpoint-1
Incident graph
Timeline
Detections
Computers
Executables
Processes
Incident
Timeline
Assistant
detection_trigger.exe (1496)
explorer.exe (5848)
notepad.exe (6648)
memoryscannertestfile.exe
ei- -mgr-test-endpoint-1
ei- -mgr-t\administrator
%commonprograms%\accessories\notepad.lnk
make-nearmiss.exe (3244)
executor.exe
What data or information was accessed or exfiltrated?
The data accessed or exfiltrated includes a dropped executable named make-nearmiss.exe, which was flagged as similar to known malware but not confirmed as malware yet. Additionally, suspected botnet activity with the threat name Win32/BotnetProtectionTest was detected from source IP 127.0.0.1 to destination IP 127.0.0.1, initiated by the user ei- -mgr-t\administrator through httpclienttester.exe, which was blocked due to its unknown reputation and lack of signature.
IMPORTANT: Generated by AI. Verify information for accuracy.
What is the reputation of the dropped executable make-nearmiss.exe?
The dropped executable make-nearmiss.exe has a reputation of "trusted."
IMPORTANT: Generated by AI. Verify information for accuracy.
any more suggestions?
1. Can you provide more details about the source IP 127.0.0.1 and the destination IP 127.0.0.1 in the suspected botnet activity?
2. What action was taken in response to the suspected botnet activity with the threat name Win32/BotnetProtectionTest?
3. Can you provide information about the process httpclienttester.exe and its reputation?
IMPORTANT: Generated by AI. Verify information for accuracy.
Ask ESET AI Advisor anything...
Responses are generated by AI. Verify information for accuracy.
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
GRAPH

How to effectively defend?



Basic measures and processes

The need to implement and adopt basic security measures, such as **limiting services available from the Internet, network segmentation, patching applications/OS, use and secure management of service accounts,** robust **backups**, **user training,** and last but not least,
Operational and safety monitoring



Learn from the mistakes of others

Fragments from the investigation

Brute force

A month-long attack with no response from administrators

Vulnerabilities

Publicly available server with 3 critical vulnerabilities

Update

Deployed 7-year-old versions of the anti-malware system

Self-defense

Safety products without tamper protection

Backups

All backups on a NAS accessible from the Internet

Monitoring

5 days without responding to non-functional anti-malware protection

Remote Encryption | The need to protect all devices

Security audit / pentest

Assessment of the level of security, evaluation of compliance with relevant requirements and practical verification of exploitability of security vulnerabilities



The need to detect new threats

Primarily **attacks that exploit legitimate system tools, scripts, and built-in operating system functions** in manual attacks



Using the EDR/XDR system

ESET XDR enables the detection, investigation and elimination of manual attacks based on the detection of potentially risky anomalies

- When exploiting operating system functions
- Within third-party apps
- In user behavior
- In network traffic



HealthCheck

Identify weaknesses in ESET platform settings and then help with optimal configuration recommendations



Do we have high-quality security technologies capable of protecting us?

Do we have high-quality security technologies capable of protecting us?

Do we have someone who will check the infiltration in the event of an attack and neutralize the threat in time?

ESET MDR | Cyber Surveillance Service

Outsourcing of missing security specialists



The most advanced safety technologies



Leading Cyberattack Experts



24/7 monitoring with response time up to 1 minute



Protect against advanced threats

ESET for SOC

ESET Research | Prague | eCrime Unit

Newly created team of cybercrime research specialists with a primary focus on ransomware groups

- A five-member team of researchers from the viruslab in the Prague center
- Global focus, cooperation with other R&D centers
- In-depth analyses of security incidents
- Dual-Use Tool Analysis
- Monitoring of the darknet and communication channels of cybercriminals
- Improving ESET AV, XDR and MDR Detection Procedures
- Notify customers of an ongoing attack

welivesecurity BY eset

ESET Research

CosmicBeetle steps up: Probation period at RansomHub

CosmicBeetle, after improving its own ransomware, tries its luck as a RansomHub affiliate

Jakub Souček
10 Sep 2024 , 25 min. read



ESET researchers have mapped the recent activities of the CosmicBeetle threat actor, documenting its new ScRansom ransomware and highlighting connections to other well-established

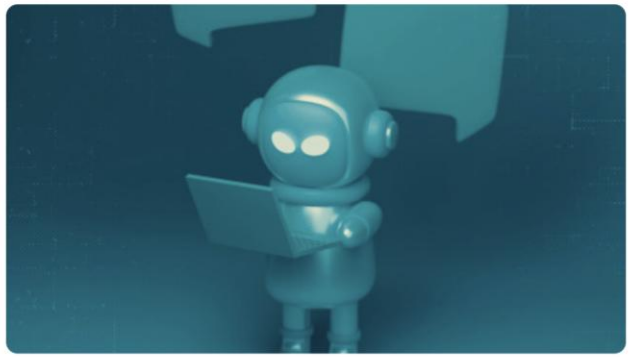
welivesecurity BY eset

ESET Research

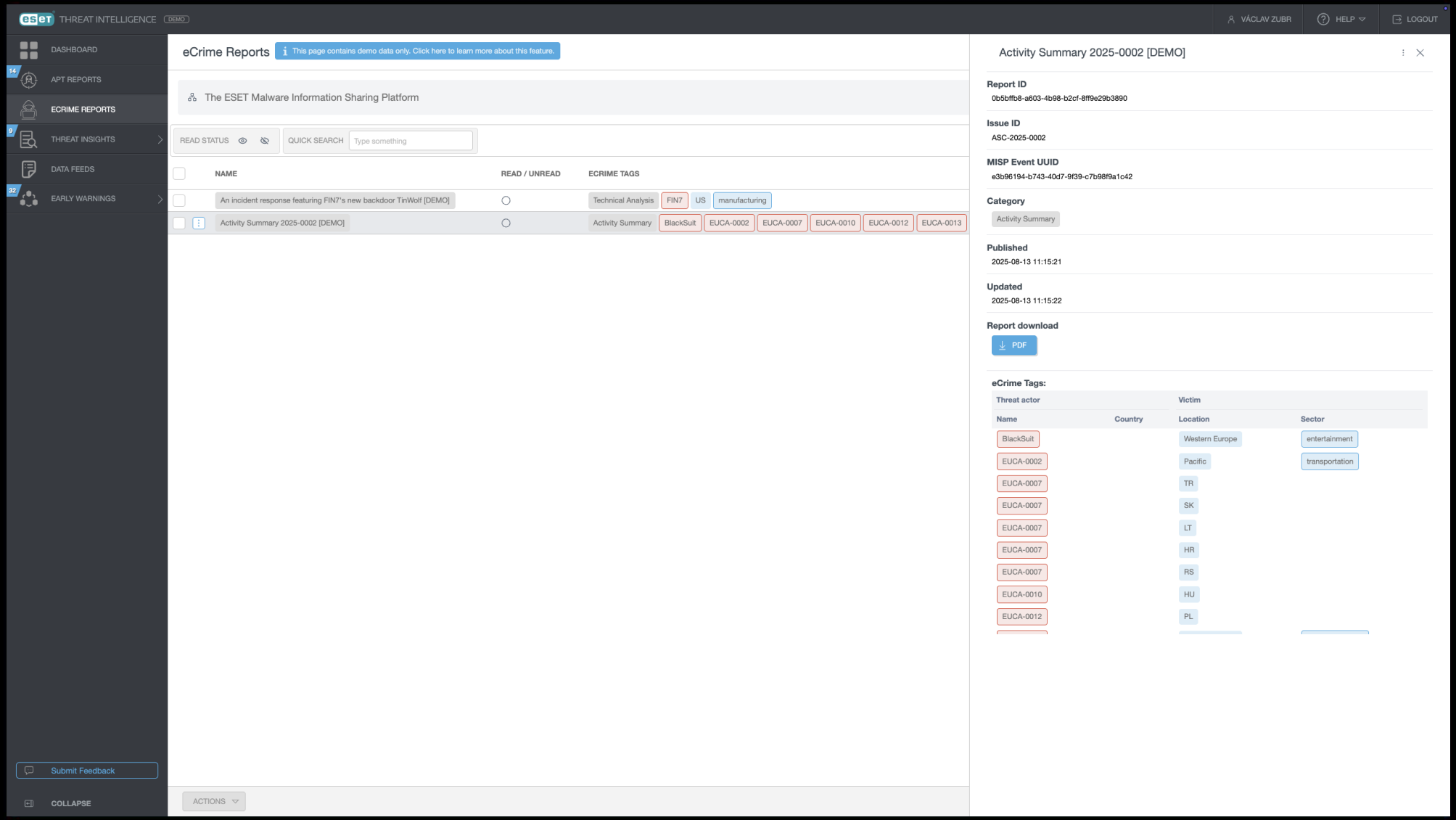
First known AI-powered ransomware uncovered by ESET Research

The discovery of PromptLock shows how malicious use of AI models could supercharge ransomware and other threats

Anton Cherepanov, Peter Strýček
26 Aug 2025 , 2 min. read



UPDATE (September 3rd, 2025): ESET Research has been contacted by the authors of an academic study


eset THREAT INTELLIGENCE DEMO
VÁCLAV ZUBR
HELP
LOGOUT
DASHBOARD
APT REPORTS
14
ECRIME REPORTS
THREAT INSIGHTS
9
DATA FEEDS
EARLY WARNINGS
32
Submit Feedback
COLLAPSE
eCrime Reports
This page contains demo data only. Click here to learn more about this feature.
The ESET Malware Information Sharing Platform
READ STATUS
QUICK SEARCH
Type something
NAME
READ / UNREAD
ECRIME TAGS
An incident response featuring FIN7's new backdoor TinWolf [DEMO]
Technical Analysis
FIN7
US
manufacturing
Activity Summary 2025-0002 [DEMO]
Activity Summary
BlackSuit
EUCA-0002
EUCA-0007
EUCA-0010
EUCA-0012
EUCA-0013
ACTIONS
Activity Summary 2025-0002 [DEMO]
Report ID
0b5bffb8-a603-4b98-b2cf-8ff9e29b3890
Issue ID
ASC-2025-0002
MISP Event UUID
e3b96194-b743-40d7-9f39-c7b98f9a1c42
Category
Activity Summary
Published
2025-08-13 11:15:21
Updated
2025-08-13 11:15:22
Report download
PDF
eCrime Tags:
Threat actor
Victim
Name
Country
Location
Sector
BlackSuit
Western Europe
entertainment
EUCA-0002
Pacific
transportation
EUCA-0007
TR
EUCA-0007
SK
EUCA-0007
LT
EUCA-0007
HR
EUCA-0007
RS
EUCA-0010
HU
EUCA-0012
PL



1


2


3


4


5



ESET Threat Intelligence reports PREMIUM

TLP: AMBER+STRICT

Digital Security
Progress. Protected.

TECHNICAL ANALYSIS

eCrime

An incident response featuring FIN7's new backdoor TinWolf

Issue:

TAC-2025-0002 v1.0

1 January, 2025

(eset):research

* This report and its contents have been provided for distribution within your organization only. Downloaded on 2026-03-09 13:28:57 by customer cf564f0a.

ESET | eCrime reports

Up-to-date, verified and unique information on real cyberattacks

- Learn about new ransomware and infostealer campaigns
- Monitoring of attack groups and analysis of their ways of operating
- A detailed overview of new techniques, tactics and procedures of attackers
- Analysis of the attack infrastructure and tools used
- Practical recommendations for prevention and response
- Data feeds with IoC for automated detection
- Access ESET MISP for data synchronization
- ESET LiveAI Assistant for contextual analysis and reporting

Access to exclusive intelligence on

APT groups

"Your reports on Chinese APTs are better than those from Mandiant."

Threat intelligence analyst, ESET Thrteat Inteligence (ETI) customer

Vladimír Čapek | Solution Architect

vladimir.capek@eset.com

