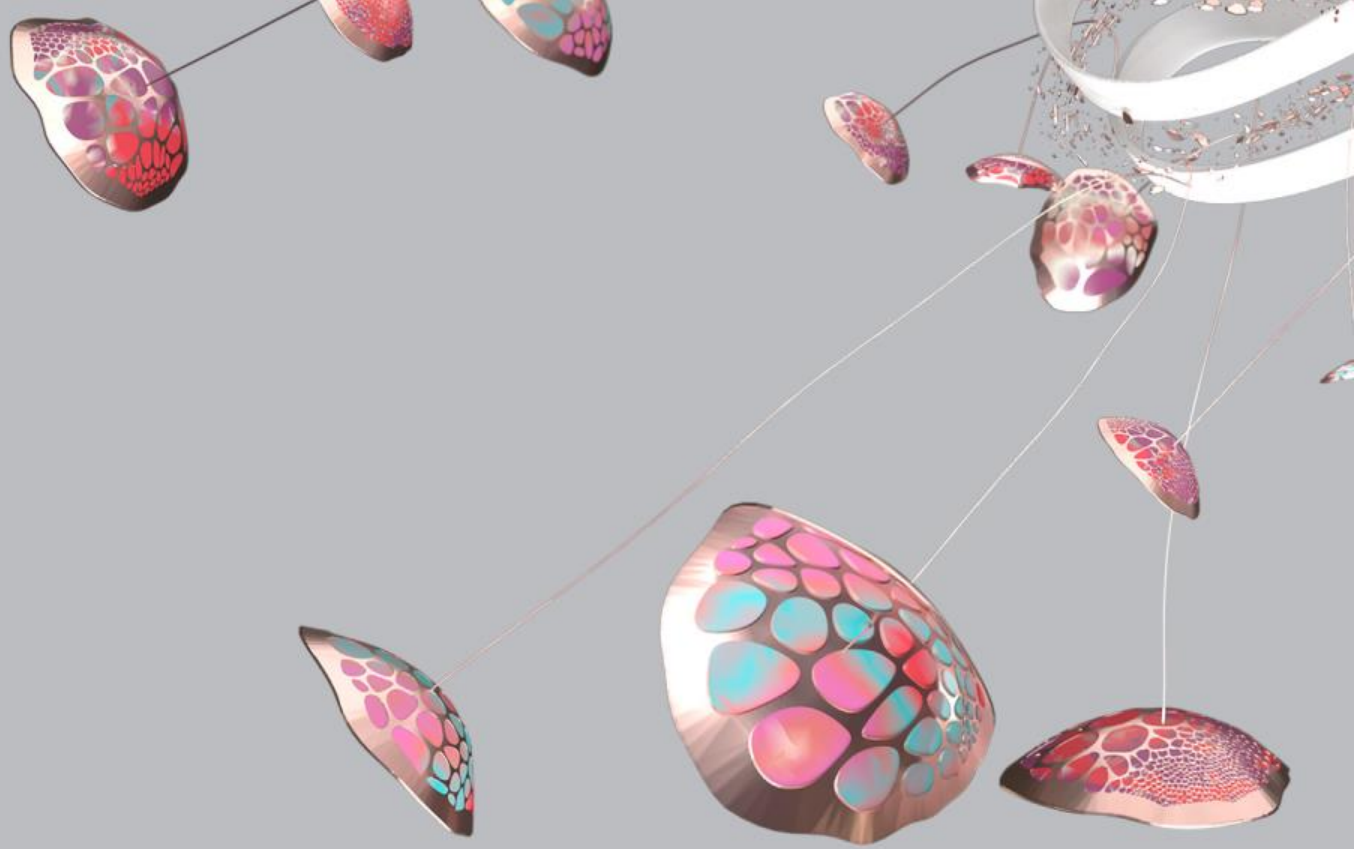


Proč?!?

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:

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 (@n0psledbyte), 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!

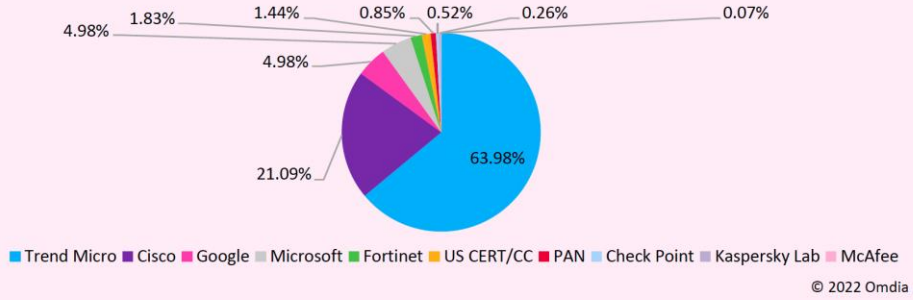
PWN2OWN TORONTO 6.-8.12.2022

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
TP-Link AX1800 WiFi 6 Router (Archer AX21)	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
NETGEAR Nighthawk WiFi6 Router (RAX30 AX2400)	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
Synology RT6600ax	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
Cisco Integrated Service Router C921-4P	WAN Side	$30,000 (USD)	3
	LAN Side	$15,000 (USD)	2
Mikrotik RouterBoard RB2011UiAS-IN	WAN Side	$30,000 (USD)	3
	LAN Side	$15,000 (USD)	2
Ubiquiti Networks EdgeRouter X SFP	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
Grand total	**1,543**	**7.49**	**2.25**	**5.12**

Figure 1: Number of vulnerabilities by CVSS severity

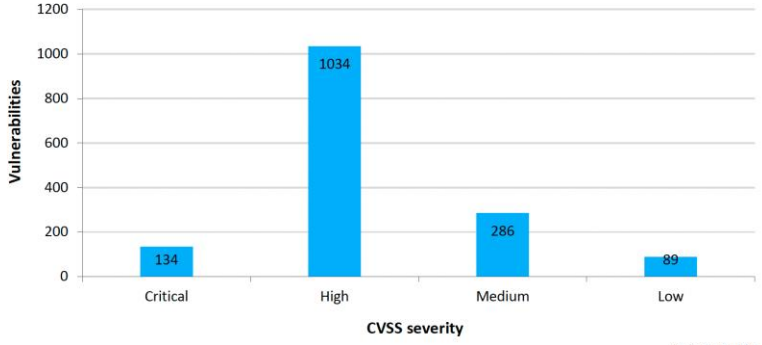
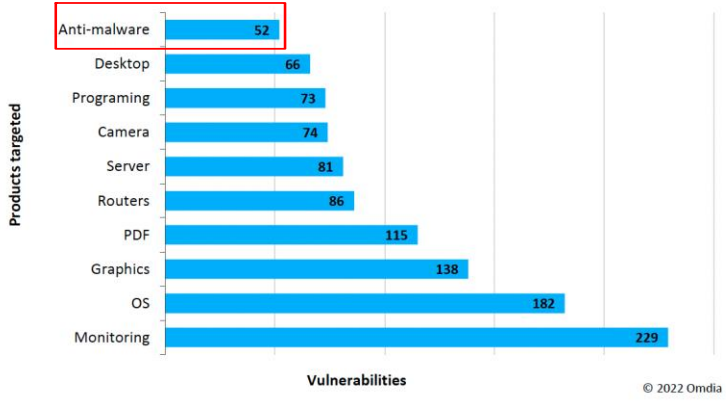
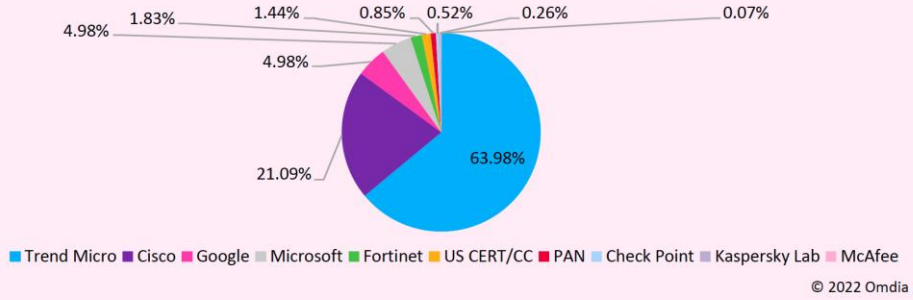


Figure 2: Number of vulnerabilities by type of products targeted



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
Grand total	**1,543**	**7.49**	**2.25**	**5.12**

Figure 4: Number of high vulnerabilities by contributor

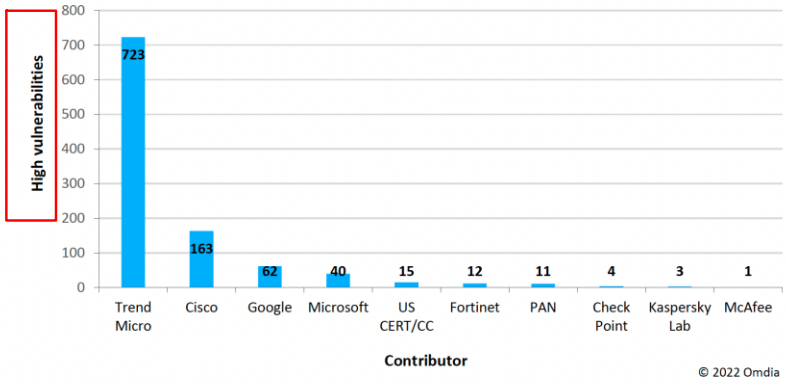
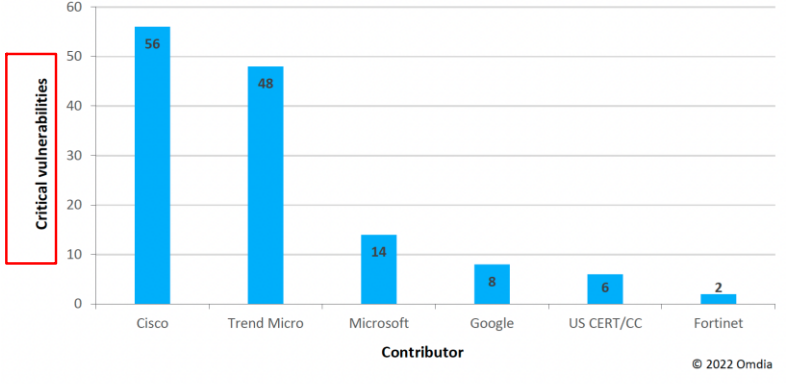
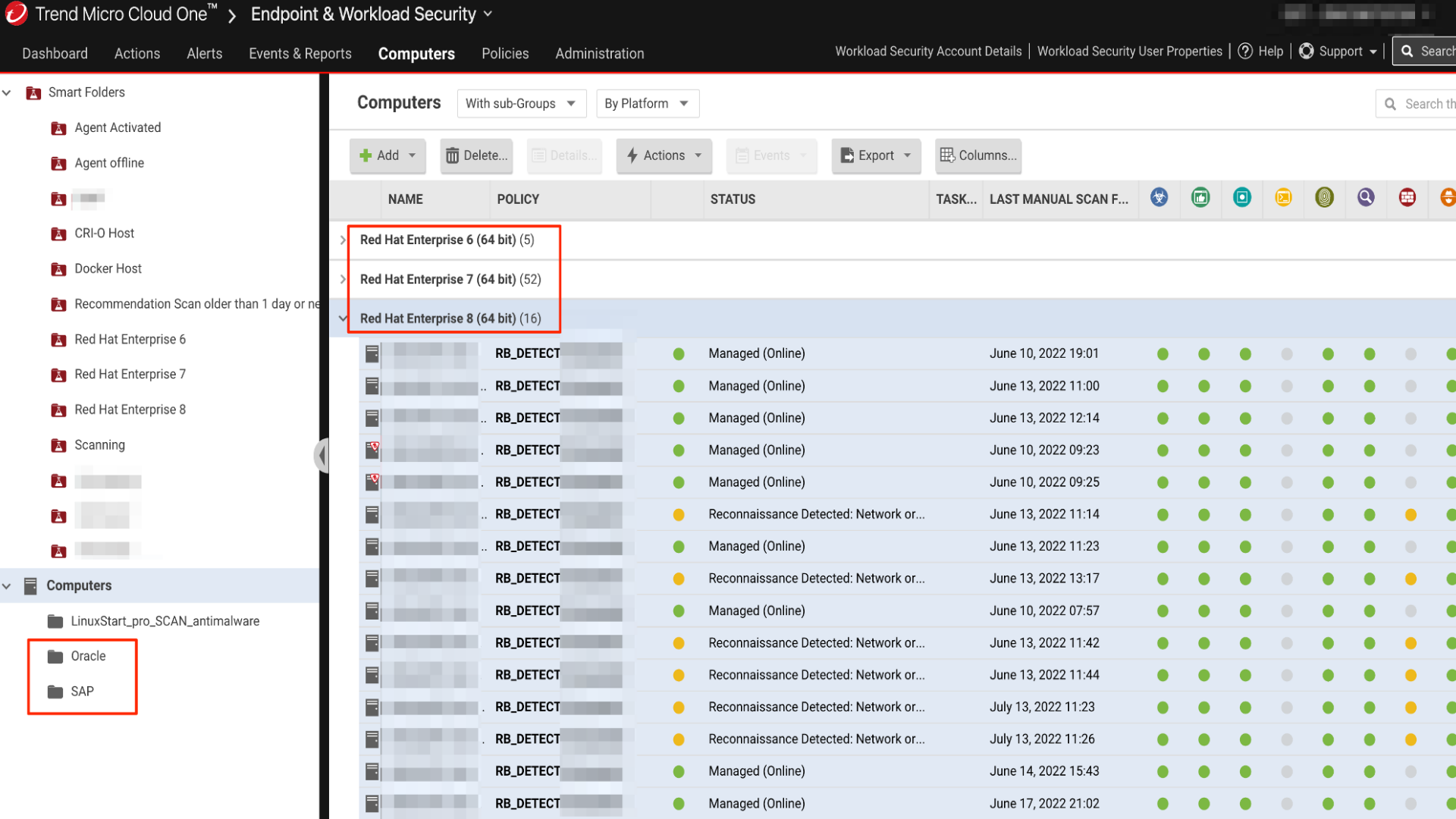
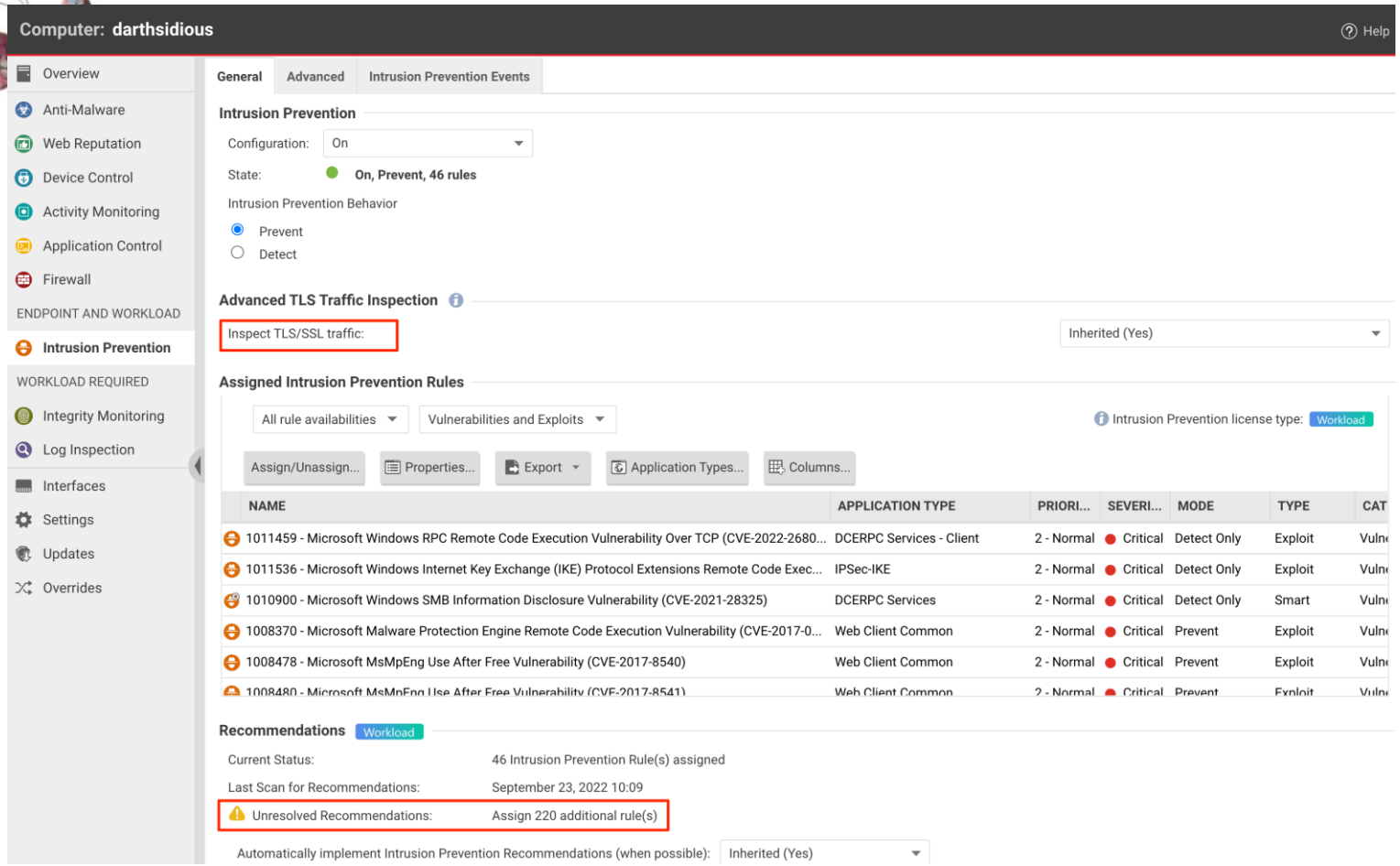


Figure 3: Number of critical vulnerabilities by contributor




Trend Micro Cloud One™ > Endpoint & Workload Security
Dashboard
Actions
Alerts
Events & Reports
Computers
Policies
Administration
Workload Security Account Details | Workload Security User Properties | Help | Support | Search
Smart Folders
Agent Activated
Agent offline
CRI-O Host
Docker Host
Recommendation Scan older than 1 day or ne
Red Hat Enterprise 6
Red Hat Enterprise 7
Red Hat Enterprise 8
Scanning
Computers
LinuxStart_pro_SCAN_antimalware
Oracle
SAP
Computers
With sub-Groups
By Platform
Search th
Add
Delete...
Details...
Actions
Events
Export
Columns...
NAME
POLICY
STATUS
TASK...
LAST MANUAL SCAN F...
Red Hat Enterprise 6 (64 bit) (5)
Red Hat Enterprise 7 (64 bit) (52)
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



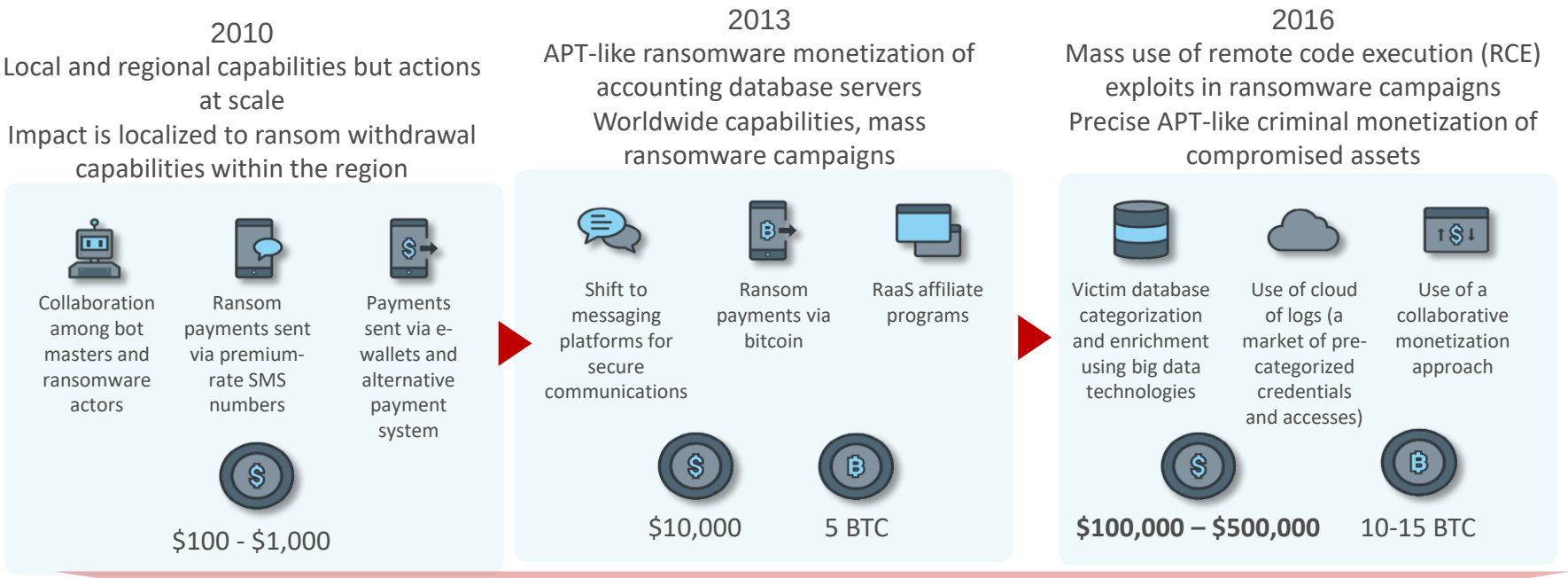
Ransomware Disrupts Critical Infrastructure

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.

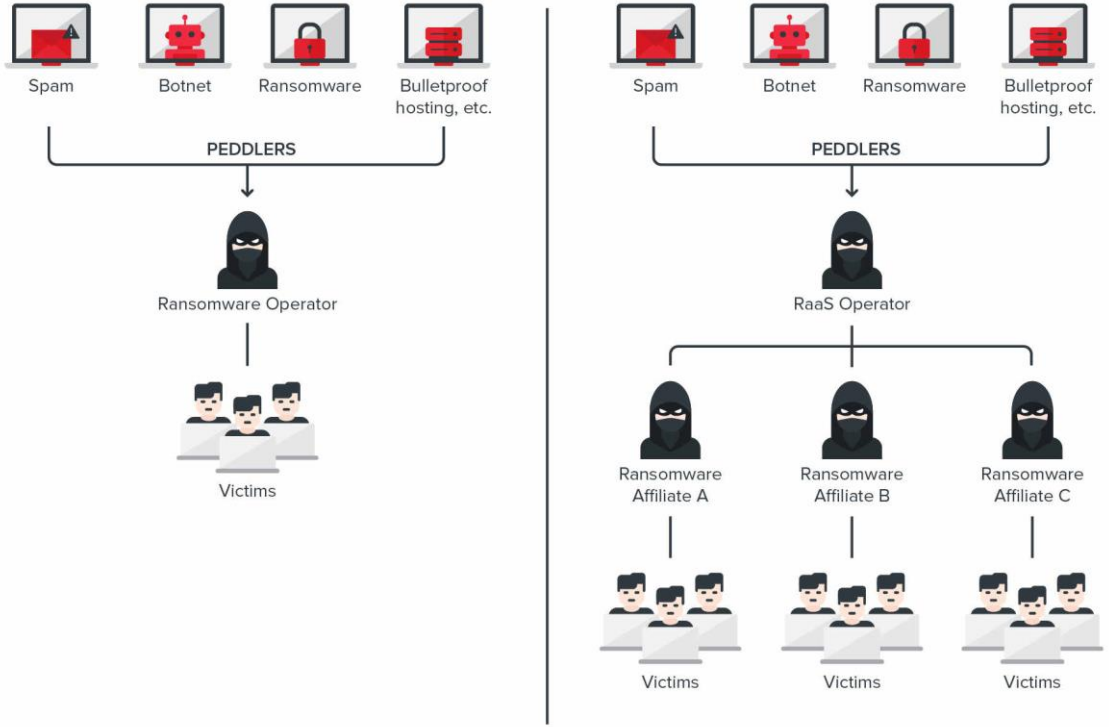
Ransomware Business Process



2021

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

How RaaS Operates



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

TREND MICRO

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

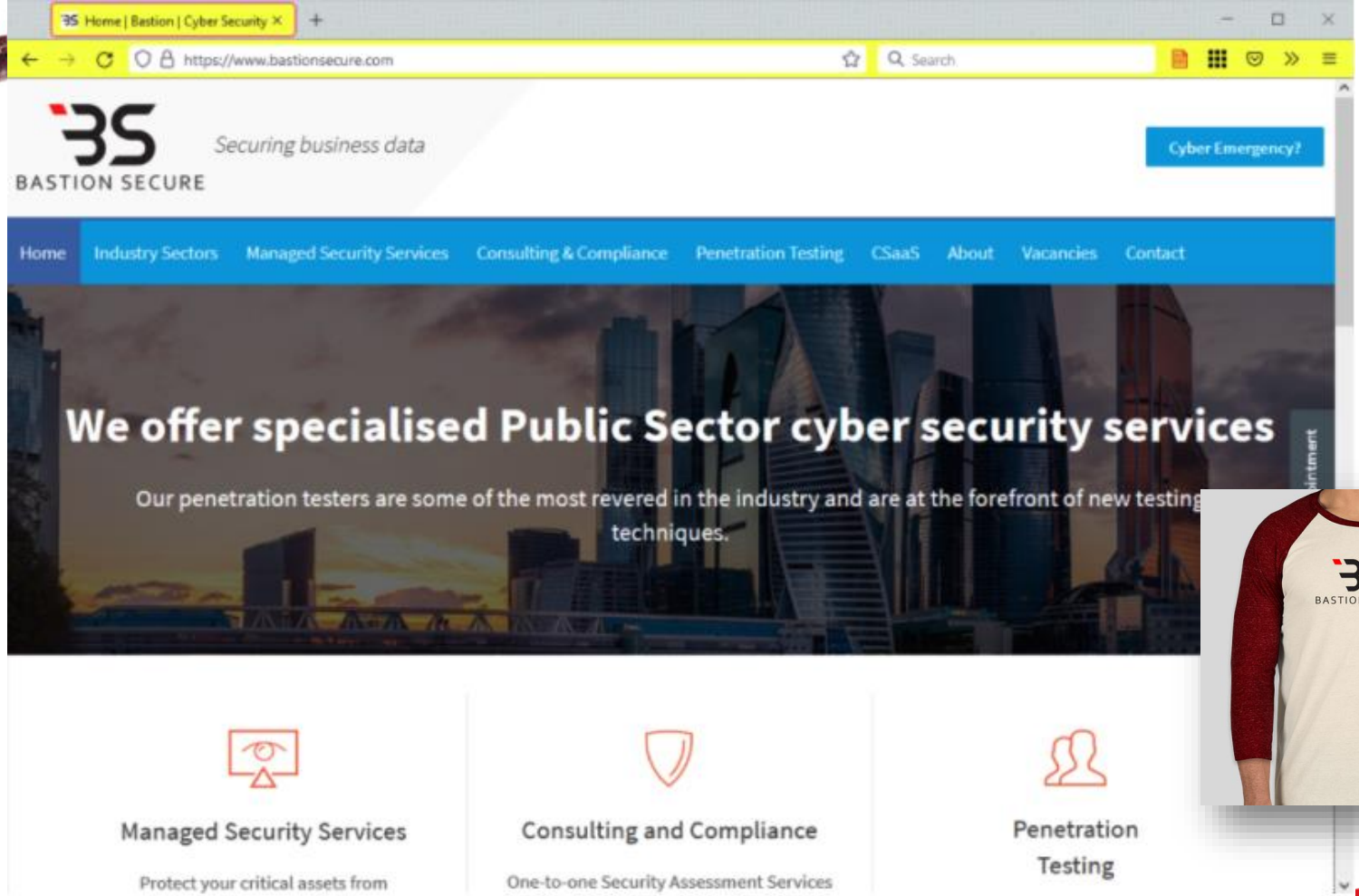
They sell access to other malicious actors

80% of the profit goes to the ransomware group

20% goes to the access broker

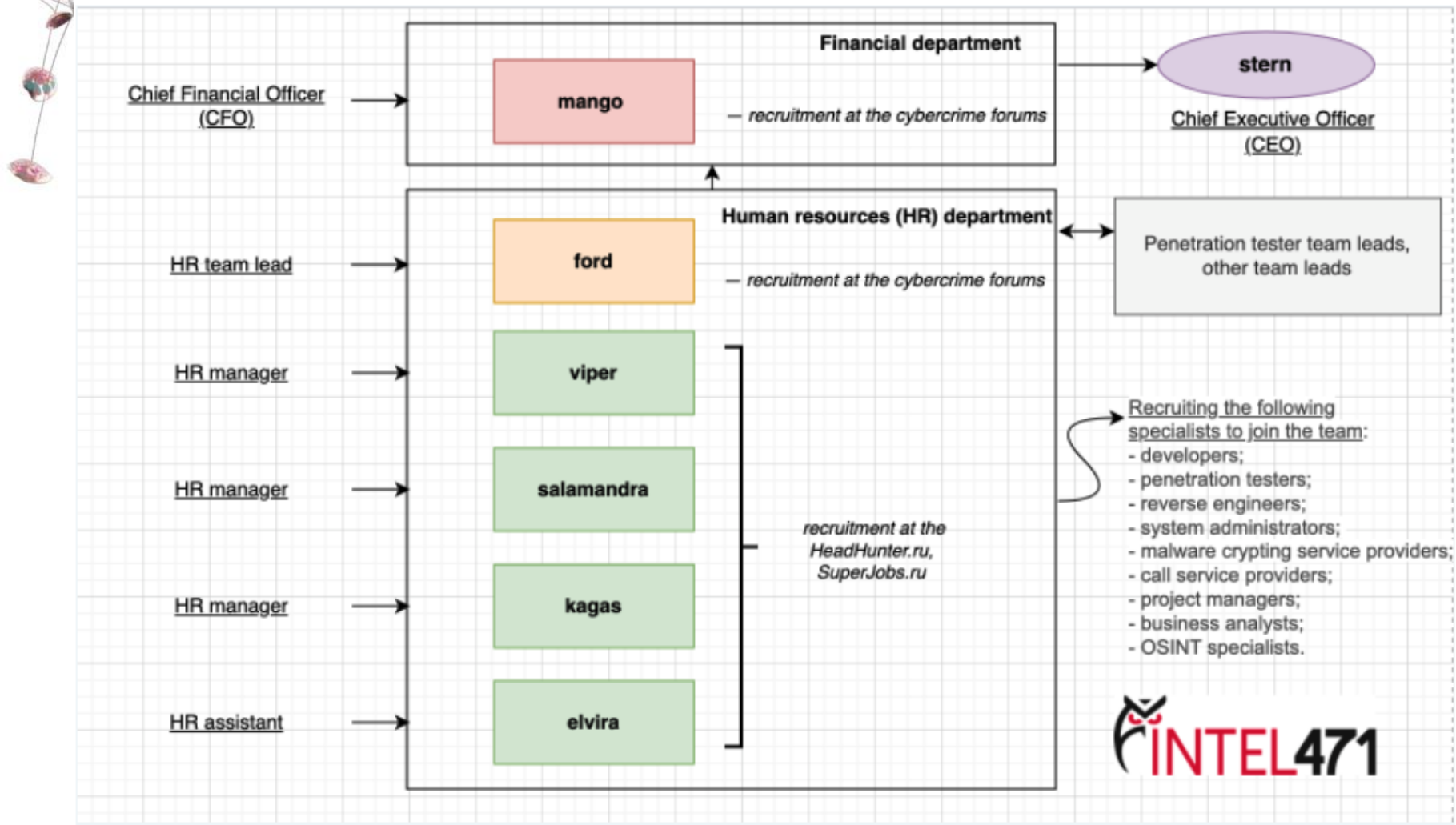
New Ransomware Evolution

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



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

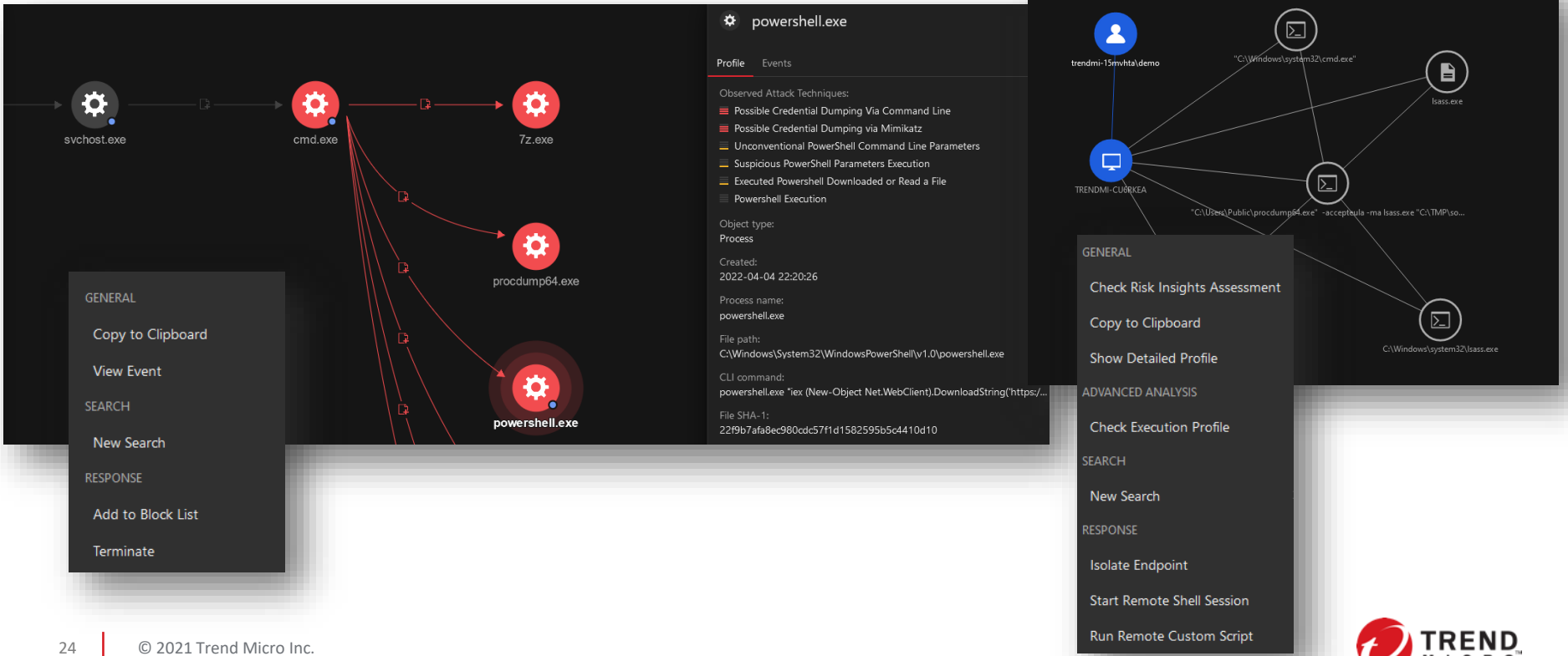
Source: intel471



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

Endpoint Detect Response

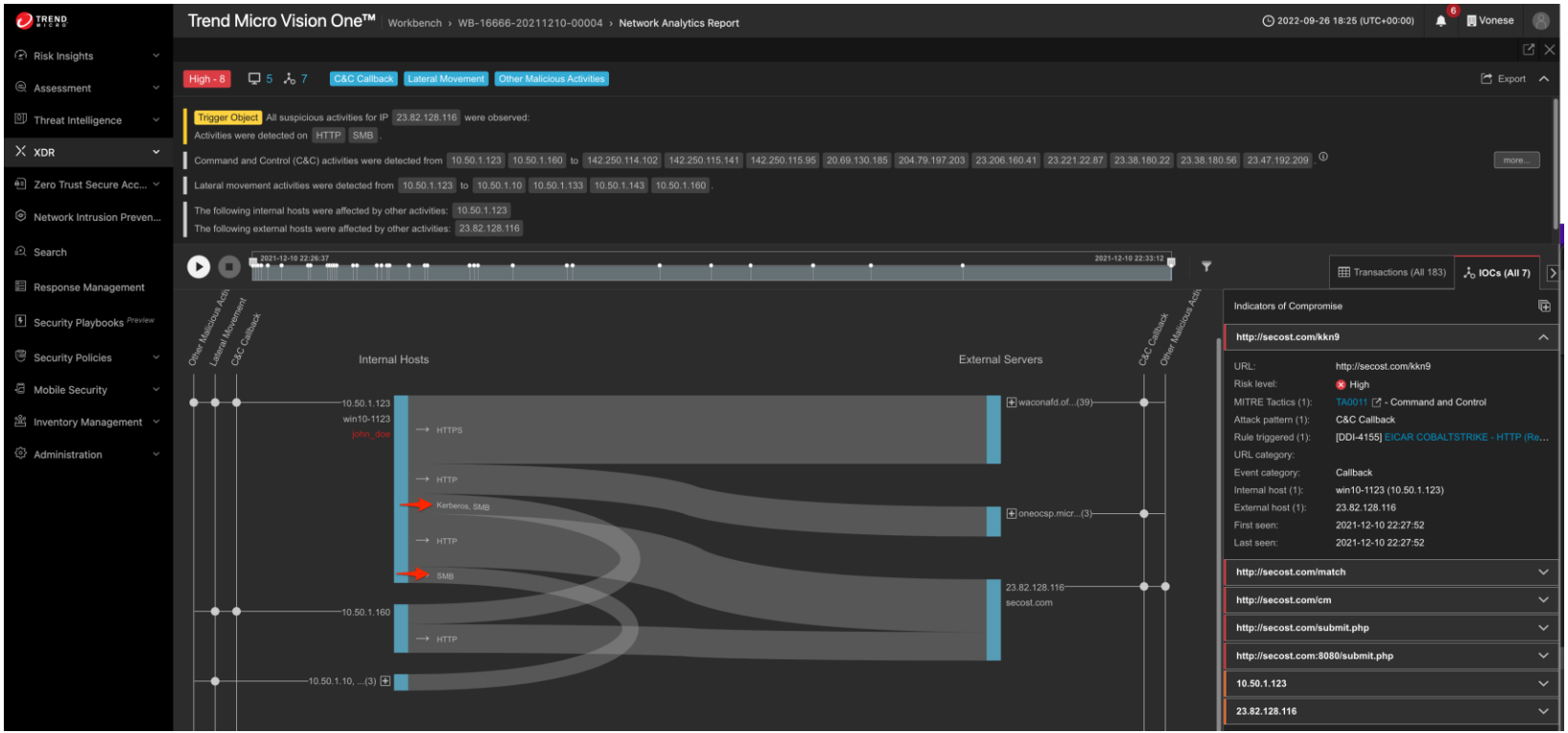
- **Stálý** sběr **veškerých** relevantních událostí na endpointech
- **Response akce**, které vám umožní rychle reagovat na probíhající událost (**remote shell**, **run custom script**, izolace agenta, záloha operační paměti, blokace, uložení souboru, soubor do sandboxu, …)
- **Retence EDR dat za půl 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!**



Network Detect Response

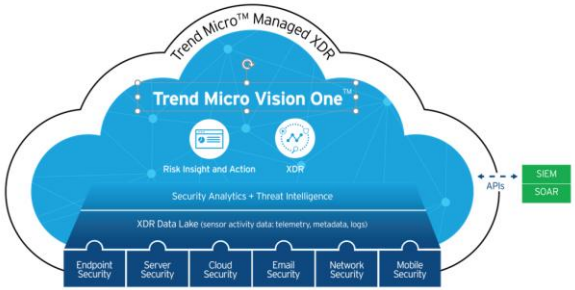
- Analýza síťového provozu **včetně inspekce aplikační vrstvy** a co největšího množství protokolů (samotné NetFlow je dost málo)
- **Produkt postavený na vykradení Virus Total databáze s „umělou inteligencí“ fakt nic neřeší!** - chytání exploitů, JA3/JA3S hash TLS spojení, kolikrát byla aplikace viděna 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



3. Sandbox – častěji jako nástroj SOCu

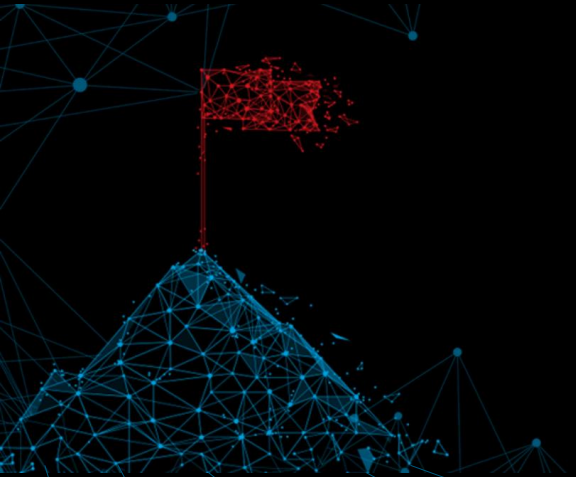
- Možnost plné konfigurace virtuálního prostředí
  - Vlastní jazykové verze
  - Možnost instalace vlastních aplikací, podpora libovolného typu souboru
  - Desktopové i serverové operační systémy, Windows, Linux, MacOS
  - V praxi i 300MB soubor (který v zipu má 20KB)
- Funkce interaktivního spuštění 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