

# Collect, Detect, Respond

**A SIEM built for threat intelligence**



# Who is Perch?

## What is Perch?

- Managed Threat Detection & Response
- SIEM
- SOC as a Service

## Powered by Industry Specific Threat Intelligence

- OT and ICS Specific Threats
- Powered by industry specific threat intelligence:
- OT and ICS specific threats
- Highly curated intelligence from reputable sources like DHS

## Executive team:

Threat intelligence pioneers and security experts

## Partnerships:

MM, FS, H, Water, MTS, and Retail ISACs

Multiple ISAOs (MPS, CU)

## Rapid platform adoption:

Thousands of customers over 1 million endpoints secured

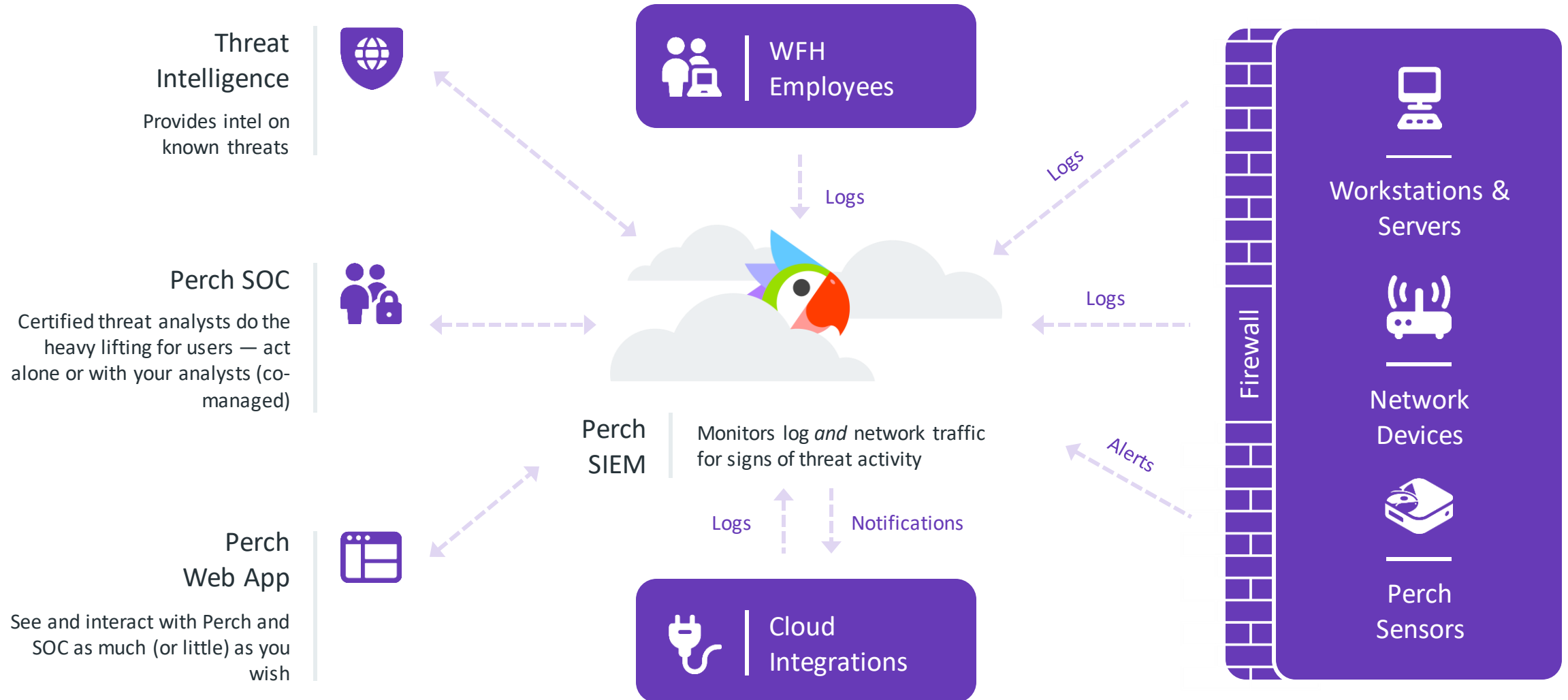


# Things You Can Do With Perch

- Get true security monitoring 24x7x365 for all sources of data anywhere they exist [especially critical during pandemic]
- Solve for cloud-based threats like account takeovers, data leaks, and access monitoring
- Maintain full threat visibility across IT and OT environments
- Augment your own SOC in tier 1 triage of threat detection



# How Perch Works



# whoami

## Paul Scott (Director of Threat Research aka Perch Labs)

- Certs
  - GWAPT
  - Advanced GWAPT
  - GSLC
  - GPEN
- Hats
  - Threat Analyst
  - Threat Hunter
  - Threat Researcher
  - Intel Analyst
  - Exploit Developer
  - Manager

## Security Content

- Turn intel into IDS signatures and SIEM rules

## Automation

- Help the SOC analyze alerts

## Research

- Find new techniques, discover campaigns, analyze malware, and document findings
- Sandbox detonation
- Honeynet lure

## Intelligence

- Threat hunt in customer data with open source intel and sandbox data



# Threat Landscape

## Threaty threat stats

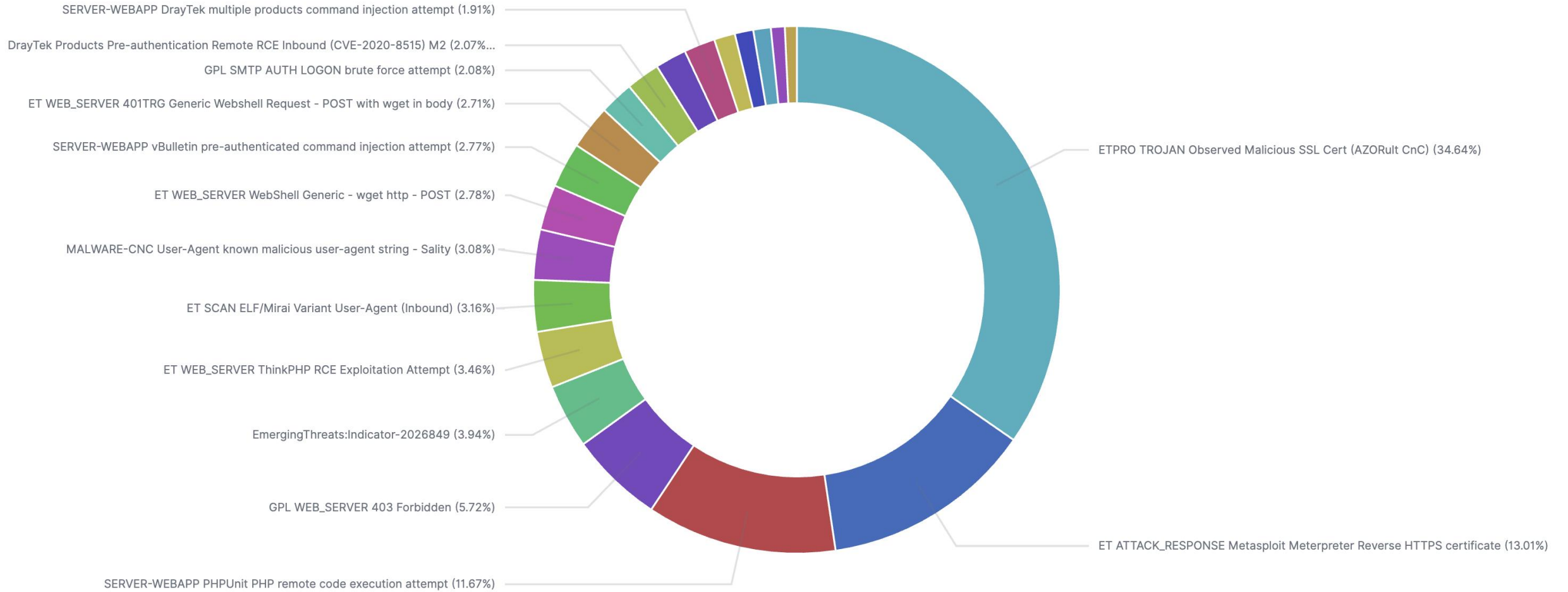
- 110,494 total alerts triaged
- 434 unique alerts triaged
- Escalation trends
  - pups, adware, trojans, unauthorized remote-control software, malicious psexec service installation, bitcoin miners, unauthorized data exfil to dropbox, pentests
- 17 Perch+Water ISAC organizations

## Topics

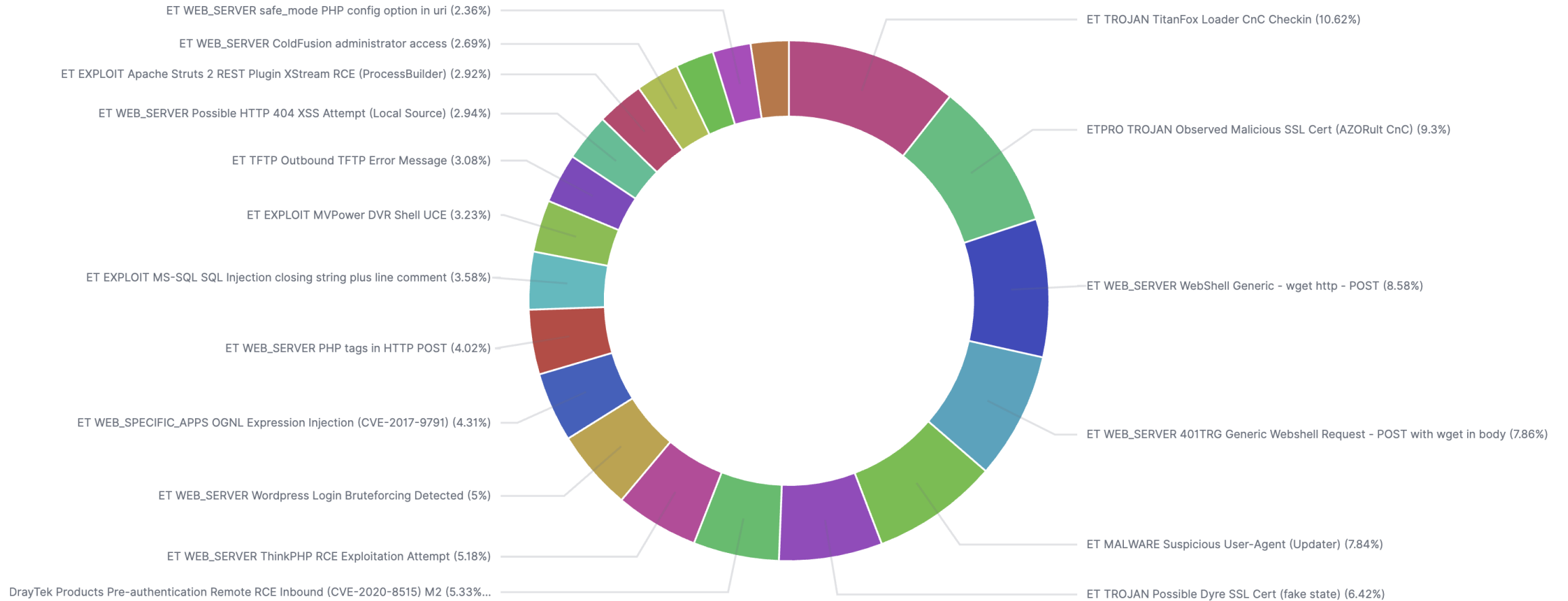
- How do Water threats compare to everyone else?
- Talking about Top Trojans
- Where are these Exploit attempts coming from?



# Top 20 Alerts Triaged For Water



# Top 20 Alerts





# Trojan IoCs

IoC description ↕	Count ↕	Unique Orgs ↕
ETPRO TROJAN Observed Malicious SSL Cert (AZORult CnC)	5,754	2
ETPRO TROJAN Win32/Fadok.A Checkin	319	1
ET TROJAN Possible Upatre Downloader SSL certificate (fake loc)	46	1
ET TROJAN Possible Upatre Downloader SSL certificate (fake org)	32	1
ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses	12	2
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	10	1
ET TROJAN Injected WP Keylogger/Coinminer Domain Detected (cloudflare .solutions in DNS Lookup)	10	1
ET TROJAN CobaltStrike DNS Beacon Response	9	1
ET TROJAN Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-2	8	1
ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1	8	1
ETPRO TROJAN Win32/Megalodon/AgentTesla Conn Check	7	1
ET TROJAN Self-Signed Cert Observed in Various Zbot Strains	6	1
ET TROJAN Double HTTP/1.1 Header Inbound - Likely Hostile Traffic	5	2
ET TROJAN Backdoor family PC RAT/Gh0st CnC traffic	4	2
ET TROJAN MSIL/Modi RAT CnC Command Inbound (plugin)	4	1
ET TROJAN Possible Windows executable sent when remote host claims to send html content	3	2
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)	2	1
ET TROJAN Backdoor family PC RAT/Gh0st CnC traffic (OUTBOUND) 106	2	1
ET TROJAN Generic DNS Query for Suspicious CryptoWall (crpt) Domains	2	1
ET TROJAN Possible Dridex SSL Cert Aug 12 2015	2	1
ET TROJAN Possible Windows executable sent when remote host claims to send a Text File	2	1
ETPRO TROJAN Observed Malicious SSL Cert (MageCart CnC)	2	1
ET TROJAN Backdoor.Win32.RShot Ping Outbound	1	1
ET TROJAN Netwire RAT Client HeartBeat	1	1
ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)	1	1
ET TROJAN Suspicious Download Setup_ exe	1	1
ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND	1	1
ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)	1	1
ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)	1	1
ETPRO TROJAN TinyLoader.C CnC Beacon x86	1	1
ETPRO TROJAN Win32/Quervar.C Possible NetBIOS Query (KASPERSKY)	1	1



# Exploit IoCs

IoC description	Count	Unique Orgs
ET EXPLOIT Multiple DrayTek Products P	344	4
ET EXPLOIT MVPower DVR Shell UCE	178	3
ET EXPLOIT Zyxel NAS RCE Attempt Inb	141	4
ET EXPLOIT Multiple DrayTek Products P	119	3
ET EXPLOIT [401TRG] ZeroShell RCE Inb	97	2
ET EXPLOIT Joomla RCE M3 (Serialized I	69	3
ET EXPLOIT Netgear DGN Remote Comm	69	2
GPL EXPLOIT Microsoft cmd.exe banner	56	1
ET EXPLOIT MS-SQL SQL Injection closin	46	1
ET EXPLOIT HackingTrio UA (Hello, Worl	42	3
ET EXPLOIT [NCC GROUP] Possible Blue	28	1
ET EXPLOIT D-Link Devices Home Netw	25	2
ET EXPLOIT Apache Struts Possible OGN	24	2
ET WEB_SPECIFIC_APPS Horde 3.0.9-3.1	14	1
ET EXPLOIT Apache Struts getWriter and	13	2
ET EXPLOIT Apache Struts memberAcce	13	2
ET EXPLOIT Apache Struts memberAcce	13	2
ET EXPLOIT Possible TLS HeartBleed Un	10	1
ET EXPLOIT Mikrotik Winbox RCE Attempt	9	3
ET EXPLOIT COMTRENAD ADSL Router C	6	3
ET EXPLOIT D-Link Router DNS Changer	6	3
ET EXPLOIT Generic ADSL Router DNS C	6	3
ET EXPLOIT Possible ShuttleTech 915WM	6	3
GPL EXPLOIT ISAPI .ida access	6	2
GPL EXPLOIT iissamples access	6	2
ET EXPLOIT Linear eMerge E3 Unauthen	5	2
ET EXPLOIT MVPower DVR Shell UCE MS	5	2
ET EXPLOIT Possible OpenSSL HeartBleed Large Heartbeat response from Common SSL Port (Outbound from Client)	5	1
ET EXPLOIT SSL excessive fatal alerts (possible POODLE attack against server)	5	1
ET EXPLOIT D-Link DSL-2750B - OS Command Injection	4	1
ETPRO EXPLOIT Adobe Acrobat Reader ACE.dll ICC mluc Integer Overflow	4	2

IoC description	Count	Unique Orgs
China	241	3
United States	214	8
Brazil	57	3
France	57	3
Indonesia	43	2
Canada	40	2
Mexico	39	3
Russia	36	3
Germany	34	2
United Arab Emirates	34	2
Italy	33	3
Colombia	31	3
Ecuador	26	2
Egypt	24	3
South Korea	22	2
Azerbaijan	21	2
Australia	18	3
India	17	3
Vietnam	16	2
Switzerland	15	1
Hong Kong	14	4
Netherlands	14	2
Panama	14	2

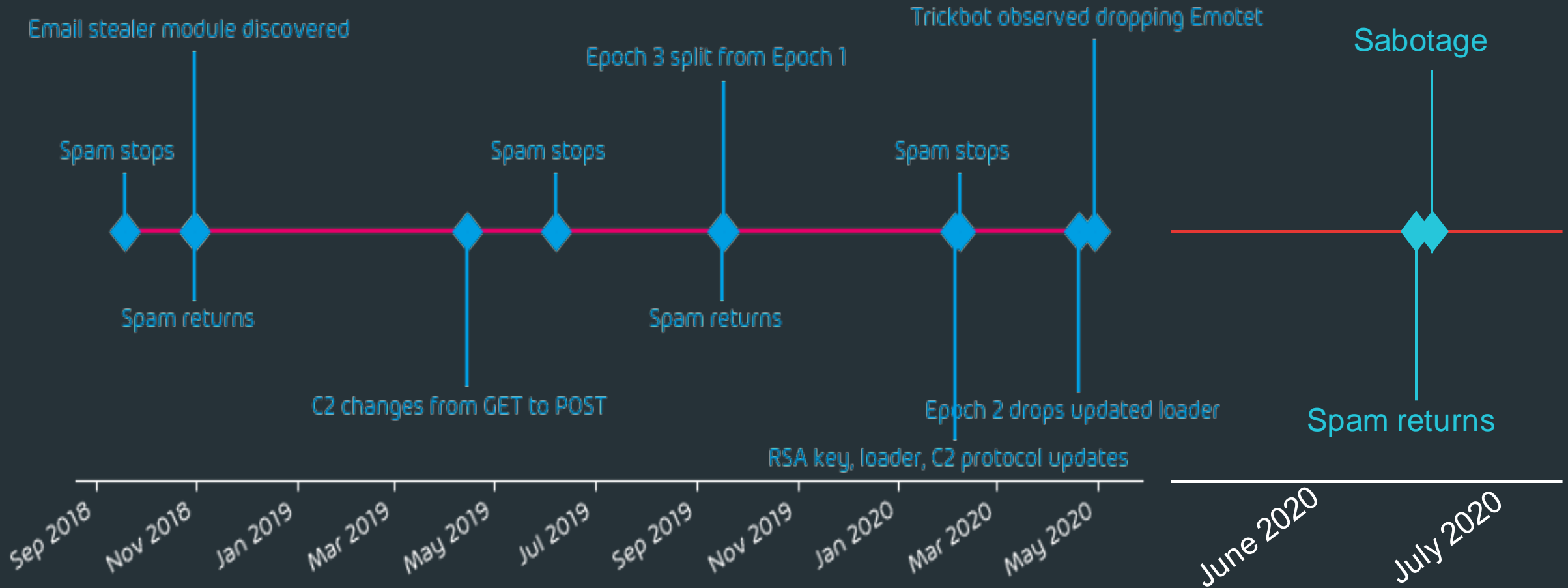


Guess who's back?

**Emotet**



# Recent Emotet Timeline



# Hack Back?



# Emotet -> Ryuk Ransomware

**DECIPHER**  
Security news that informs and inspires

Jan 11, 2019

**THE UNHOLY ALLIANCE OF EMOTET, TRICKBOT AND THE RYUK RANSOMWARE**

By Dennis Fisher







2  
f  
C

Th  
as

As we  
the th  
when  
ranso  
these  
acce  
Beac  
can d  
Rans  
lucrat

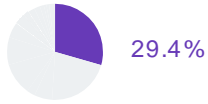
# 2020 MSP Threat Report



<https://go.perchsecurity.com/SR-2020>



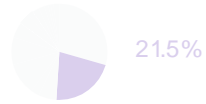




# Sodinokibi

- Sodinokibi (aka Sodin or REvil) is offered by PINCHY SPIDER in a Ransomware-as-a-Service (RaaS) model, so it is delivered by affiliates through a variety of attack vectors.
- PINCHY SPIDER launched Sodinokibi right before the retirement of GandCrab RaaS.
- Sodinokibi ransomware was first observed in April 2019 in a campaign exploiting web application vulnerabilities in Oracle WebLogic servers (CVE-2019-2725)
- A Sodinokibi ransomware campaign was also observed spreading via malvertising that leads to the RIG exploit kit. The attacks were done through advertisements on ad networks that redirected users to the browser exploit kit based on certain conditions.
- PINCHY SPIDER affiliates starting heavily targeting MSPs for Buffalo Jumps with Sodinokibi after the success of GandCrab ransomware in February 2019.

\* Average ransomware demand  
**\$71,062**



# Ryuk

- Ryuk Ransomware was developed by GRIM SPIDER as an evolution of the commodity North Korean ransomware, Hermes.
- In late 2018, Ryuk burst onto the ransomware scene with a slew of attacks on American news publications as well as government organizations.
- Targeted systems were first infected with malicious emails containing Emotet or TrickBot, two information stealing Trojans. Once a system is infected and flagged as a good target for ransomware, it is infected with Ryuk.
- Ryuk ransomware outbreaks show coordination between associated threat actor groups like MUMMY SPIDER, WIZARD SPIDER, INDRIK SPIDER, and LUNAR SPIDER

\* Average ransomware demand  
**\$779,855**



# DoppelPaymer

- DoppelPaymer was created by INDRIK SPIDER as an evolution of BitPaymer for Big Game Hunting mid 2019.
- Between May and September 2019, multiple cases were reported involving malware infection via fake browser updates. Attackers are compromising websites with fake browser updates. The fake updates appear as JavaScript alerts and entice the user to “update” in order to keep their browser running “smoothly and securely.” Then a malicious script is launched that collects information about the host computer and sends it back to the attacker’s C2 server. The server then installs malware like Dridex and laterally spreads ransomware throughout a compromised organization’s network using PSEXec.
- DoppelPaymer has also bought distribution through Emotet showing coordination with MUMMY SPIDER.

\* Average ransomware demand  
**\$102,345**



# Snatch

- Snatch Ransomware created by TOOTHY MAGPIE aka BulletToothTony and has been active since December 2018.
- Snatch offers a Ransomware-as-a-Service platform and is recruiting affiliates familiar with experience compromising RDP, VNC, and SSH services.
- In December 2019, Snatch was observed rebooting computers into “safe mode” to bypass security solutions and encrypt files once the system loads.
- TOOTHY MAGPIE affiliates are known for utilizing legitimate tools including Process Hacker, IObit Uninstaller, PowerTool, PsExec, and Advanced Port Scanner.

\* Average ransomware demand  
**\$19,500**





# PERCHLABS



[go.perchsecurity.com/share](https://go.perchsecurity.com/share)



# A Member's Perspective

Barry Blanchard, IT Manager of Onondaga County Water Authority





Barry Blanchard  
IT Manager



CHANGE FROM:  
HOW DO YOU KNOW?

TO:  
NOW YOU KNOW!

# Microsoft releases Security Updates

## **Microsoft Releases Security Updates for Windows 10, Windows Server**

Microsoft has released security updates to address vulnerabilities in Windows 10 and Windows Server. These vulnerabilities could allow a remote attacker to take control of an affected system. CISA encourages users and administrators to review the Microsoft security advisories for [CVE-2020-1425](#) and [CVE-2020-1457](#) and apply the necessary updates. [Read the advisory at CISA.](#)

WaterISAC  
sends an  
email

### **Microsoft Releases Security Updates for Windows 10, Windows Server**

Microsoft has released security updates to address vulnerabilities in Windows 10 and Windows Server. These vulnerabilities could allow a remote attacker to take control of an affected system. CISA encourages users and administrators to review the Microsoft security advisories for [CVE-2020-1425](#) and [CVE-2020-1457](#) and apply the necessary updates. [Read the advisory at CISA.](#)

Perch Threat Indicators are already in place

#### Recent Indicators

0

##### [Perch Security] PUP Activity - Suspicious Redirects

Red

Created: July 7th 2020, 5:40:59 PM UTC

Description: [Perch Security] PUP Activity - Suspicious Redirects

0

##### [Perch Security] Malware CAB File Drop

Red

Created: July 7th 2020, 5:40:59 PM UTC

Description: [Perch Security] Malware CAB File Drop

0

##### Advisory 2020-008: Copy-paste compromises - tactics, techniques and procedures used to multiple Australian networks

White

Created: July 7th 2020, 9:38:51 AM UTC

Description: Australian Cyber Security Centre Indicators of Compromise Release

0

##### [Perch Security] Valak Malware Stage 2 (license.jsp) C2


Red

Created: July 6th 2020, 8:40:14 PM UTC

Description: [Perch Security] Valak Malware Stage 2 (license.jsp) C2



An Alert is triggered if a threat is identified.


LAST SEEN	INDICATOR
hours ago	 ETPRO CURRENT_EVENTS Successful Mailbox Shutdown Phish M1 May 16 2016

# A recent notification

## WaterISAC Members:

The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have published a joint alert recommending critical infrastructure owners and operators take immediate steps to reduce exposure of operational technology (OT) and control systems at this time of heightened geopolitical tensions. While not identifying specific nation states or recent events, the alert states that civilian infrastructure makes attractive targets for foreign powers attempting to do harm to U.S. interests or retaliate for perceived U.S. aggression.

Perch allows  
us to create  
our own  
alerts

 This notification uses data for **OCWA**.

**General**

Notification Name

Description

# The Perch SOC reviews alerts to verify

After manual investigation, nothing appears malicious or unusual with the traffic. This is an INFO/Policy based alert, used for insight and context in the environment. If you have any questions or comments on this remediation, please contact us at [soc@perchsecurity.com](mailto:soc@perchsecurity.com).

A stylized, colorful parrot head logo is positioned in the bottom-left corner. It features a white eye with a black pupil, a large red beak, and a green forehead. The background of the logo consists of overlapping geometric shapes in shades of blue, purple, and green.

# Want to try Perch?

[Go.perchsecurity.com/share](https://go.perchsecurity.com/share)