# 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

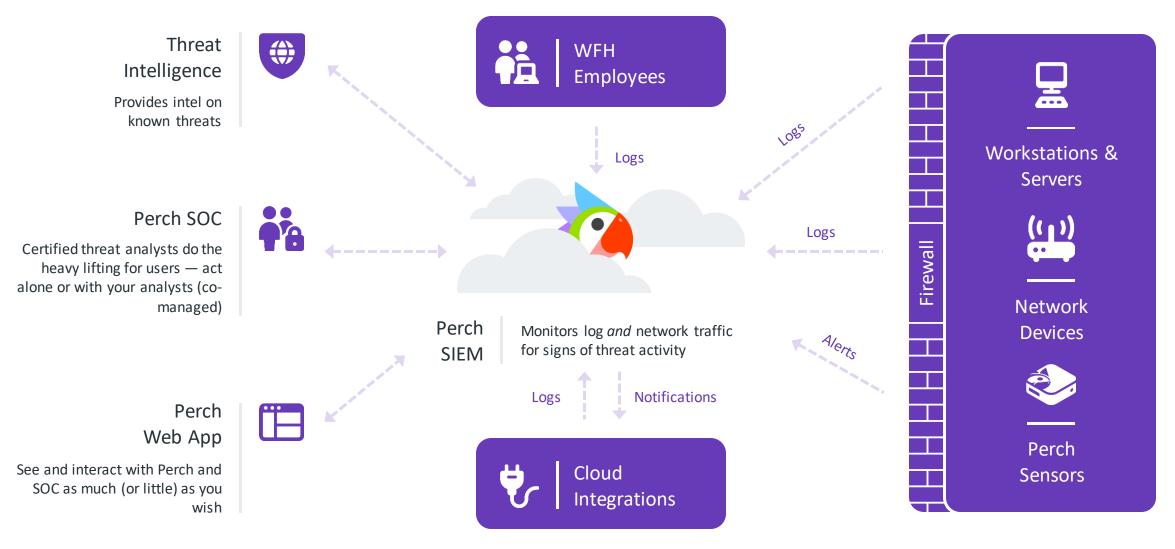


### Things You Can Do With Perch

- 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

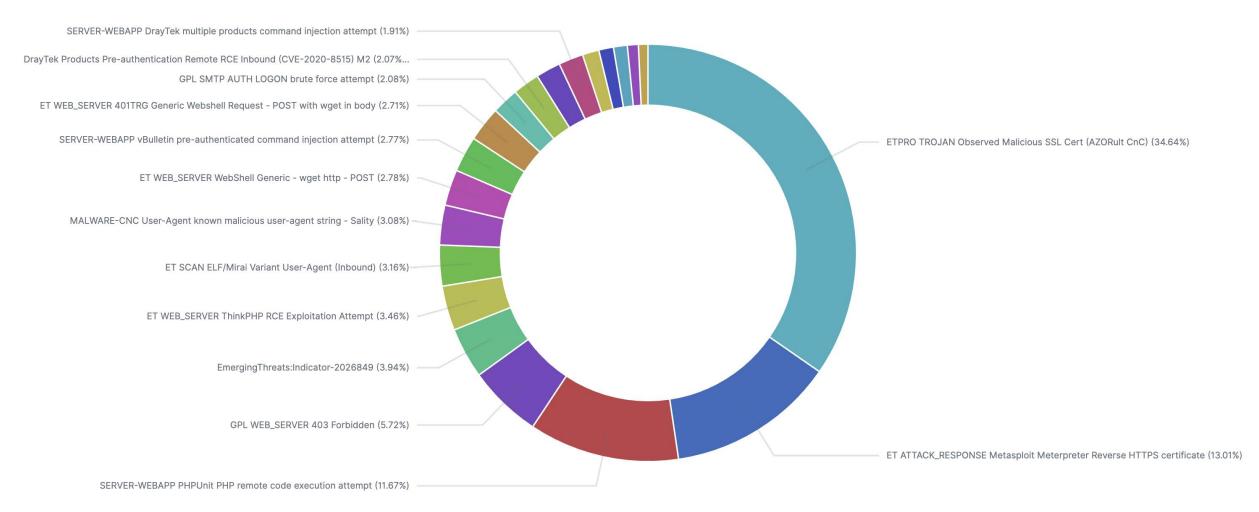
- 110,494 total alerts triaged
- 434 unique alerts triaged
- Escalation trends
  - pups, adware, trojans, unauthorized remote-control software, malicious psexec service installation, bitcoin miners, unauthorized data exfil to dropbox, pentests
- 17 Perch+Water ISAC organizations

### Topics

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

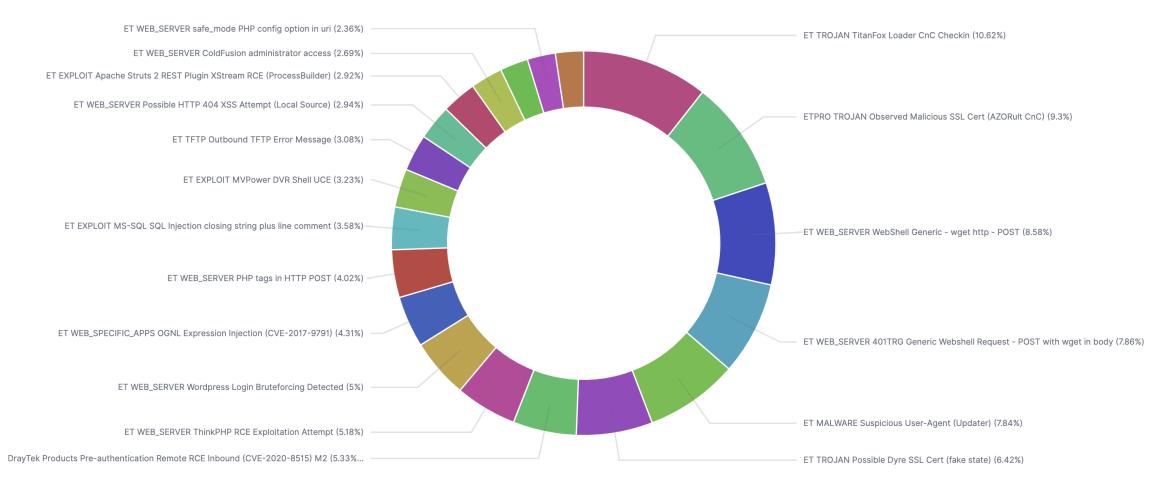


### Top 20 Alerts Triaged For Water





### Top 20 Alerts





### Trojan loCs

ETPRO TROUAN Win32/FadeA A Checkin3191ET ROUAN Win32/FadeA A Checkin461ET ROUAN Sessible Updare Downlader SSL certificate (fike org)21ET ROUAN Zeus GameOver Possible DGA NGOMAN Response101ET ROUAN RUISE CLASSL Backink Malicious SSL certificate (adeceed (fibrids))101ET ROUAN RUISE CLASSL Backink Malicious SSL certificate (adeceed (fibrids))101ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Usely Bot Nok In IRIC Country Coole S03 86-1 alpha-281ET ROUAN Self-Signed Crit Diserved In Versious S1 service In Ver	loC description ≑	Count 🗢	Unique Orgs
ET TROUAN Possible Upatre Downlader SLL certificate flake org)9491ET TROUAN Possible Upatre Downlader SLL certificate flake org)9292ET TROUAN Loss Gans/Durine Domain Detected (Didax)9291ET TROUAN Loss Gans/Durine Domain Detected (cloudiflare. scalulors in DN Lookup)991ET TROUAN Loss Cans SLL certificate dataction (Didax)9191ET TROUAN Loss SLL certificate dataction (Dirant Loss SLL certificate dataction (Didax)9191ET TROUAN SLL Certificate dataction (Dirant Loss SLL certificate dataction (Dirant Loss Certificate dataction (Diran	ETPRO TROJAN Observed Malicious SSL Cert (AZORult CnC)	5,754	2
ET TROJAN Possible Upåtre Downleader SSL certificate terter (s)2ET TROJAN Possible Upåtre Downleader SSL certificate terter (s)2ET TROJAN Possible DA NXDOMIN Responses0ET TROJAN Possible SSL Backist Malicious SSL certificate detected (Doublier a solutions in DNS Lookup)0ET TROJAN Possible Data NXDOMIN Response8ET TROJAN Possible Data Nacional SSL certificate detected (Doublier a solutions in DNS Lookup)8ET TROJAN Possible Data Nacional SSL certificate detected (Doublier a solutions in DNS Lookup)8ET TROJAN Possible Data Nacional SSL certificate detected (Doublier a solutions in DNS Lookup)8ET TROJAN Possible Data Nacional SSL certificate detected (Torent Lookup)8ET TROJAN Male Machine Country Code ISO SIME-1 alpha-28ET TROJAN Data Schoor family PCRAUChastis Traffic8ET TROJAN Maskif Malichus SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Anciena Interpose Traffic8ET TROJAN Male Machine Marker SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Marker Male Data SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Marker Male Data SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Marker Male Data SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Marker Male Data SSL certificate detected (Torent Lookup Conc)8ET TROJAN Male Machine Marker Male Data SSL certificate Detected (Torent Lookup Conc)1ET TROJAN Male Machine Marker Male Data SSL certificate Detected (Conc)1ET TROJAN Male	ETPRO TROJAN Win32/Fadok.A Checkin	319	1
ET ROJAN Zaus Gamo Over Possible DOA NXDOMAIN Response       12       2         ET ROJAN Zaus Gamo Over Possible DOA NXDOMAIN Response       10       1         ET ROJAN JUBJEC HSS, Blackisk Malicinus SS, certificate detected (obudiars solutions in NS Lookup)       10       1         ET ROJAN Universitie DOS Bescon Response       8       1         ET ROJAN Schleged Cort Oberversitie Concheck       8       2         ET ROJAN Schleged Cort Defensitie Dos Conchek       8       2         ET ROJAN Schleged Cort Defensitie Schleger Response       8       2         ET ROJAN Schleged Cort Defensitie Traffic       8       2       2         ET ROJAN AUBJECH SSL Beacht Malicious SSL certificate detected (Corter)       2       1       2       1         ET ROJAN Schleged Traffic Conches       2       1       1       1       1       1       1       1       1 </td <td>ET TROJAN Possible Upatre Downloader SSL certificate (fake loc)</td> <td>46</td> <td>1</td>	ET TROJAN Possible Upatre Downloader SSL certificate (fake loc)	46	1
ET TROJAN ABUSE,CH SSL Blacklist Malicious SSL cartificate detected (Dridex)1ET TROJAN VABUSE,CH SSL Blacklist Malicious SSL cartificate adueted (Dridex)1ET TROJAN Vasc Debatistifice DNS Blaccon Response91ET TROJAN Vasc Debatistifice DNS Blaccon Response81ET TROJAN Vasc Debatistifice DNS Blaccon Response81ET TROJAN Vasc Debatistifice DNS Discon Check71ET TROJAN Vasc Debatistifice DNS Discon Check71ET TROJAN Vasc Debatistifice DNS Discon Check62ET TROJAN Vasc Debatistifice DNS Discon Check42ET TROJAN Vasc Debatistifice DNS Discondul Usely filter32ET TROJAN Vasc Debatistifice DNS Discondul Usely filter41ET TROJAN Nasc Debatistifice DNS Discondul Usely filter32ET TROJAN Nasc Debatistifice DNS Debatistifice Debatistifice DNS Debatistifice Debatistifice DNS Debatistifice Debatistifice DNS Debatistifi	ET TROJAN Possible Upatre Downloader SSL certificate (fake org)	32	1
ET TROJAN Injected WP Keylogger/Colminer Domain Detected (cloudfare : solutions in DNS Lookup)         1           ET TROJAN CobatSrike ONS Bacon Response         9         1           ET TROJAN Likely Bot Nick in IRC (Courthy Code ISO 3166-1 alpha-2         8         1           ET TROJAN Universe         8         1           ET TROJAN Self-Signed Cert Observed in Various Zbot Strains         6         1           ET TROJAN Self-Signed Cert Observed in Various Zbot Strains         6         1           ET TROJAN Self-Signed Cert Observed in Various Zbot Strains         6         2           ET TROJAN Monother Trol Detected in Trol Detected (Distrophic Tarific         6         2           ET TROJAN Self-Signed Cert Observed in Various Zbot Strains         6         2         2           ET TROJAN Backing Mailcow Strains         6         2         2         2           ET TROJAN Backing Mailcow Strains Chart Tarific         6         2         2         2         2         2         2         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1         2         1	ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses	12	2
TROJAN ChallStrike DNS Beeon Response       9       1         ET TROJAN Likely Bot Nick in IRC (Country Code ISO 3186-1 alpha-2       8       1         ET TROJAN Unaff Variat CnC Beeon 8 M       8       1         ET RDOJAN Unaff Variat CnC Beeon 8 M       8       1         ET TROJAN Served in Various 2000 Chack       9       1         ET TROJAN Served in Various 2000 Trains       6       1         ET TROJAN Becktoor family PCRN(Vols0 CC traffic       2       2         ET TROJAN Served in Various 2000 Trains       3       2         ET TROJAN Served in Various 2000 Trains       3       2         ET TROJAN Served in Various 2000 Trains       3       2         ET TROJAN Becktoor family PCRN(Vols0 CC traffic       2       1         ET TROJAN ABUSE CH SSL Blackitst Malicious SSL certificate detected (TorrentLocker CnC)       2       1         ET TROJAN Deschoor family PCRN(Vols0 CC traffic (UTEOUND) 106       2       1         ET TROJAN Deschoor family PCRN(Vols0 CC traffic (UTEOUND) 106       2       1         ET TROJAN Deschoor family PCRN(Vols0 CC traffic (UTEOUND) 106       2       1         ET TROJAN Deschoor family PCRN(Vols0 CC traffic (UTEOUND) 106       2       1         ET TROJAN Deschoor family PCRN(Vols0 CC traffic (Vols0 CCC)       1       1	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	10	1
ET TROJAN Likely Bot Nick in IRC (country Code ISO 3166-1 alpha-2       8       1         ETPRO TROJAN Uranif Variant CnC Beacon 8 M1       7       1         ET TROJAN Sind 2/Agent East Conn Check       7       1         ET TROJAN Sind 2/Agent East Conn Check       6       1         ET TROJAN Davide ITTP/I1 leader Inbound - Likely Hostils Triffic       6       2         ET TROJAN MSIL/Modi RAT Coc Command Inbound (plugin)       4       2         ET TROJAN Backdoor family PCRAUChost Cnc traffic       3       2         ET TROJAN Backdoor family PCRAUChost Cnc Traffic (OUTBOUND) 106       2       1         ET TROJAN Backdoor family PCRAUChost Cnc Traffic (OUTBOUND) 106       2       1         ET TROJAN Davide ITTR/IN Describe Wind nemente host claims to send html content       2       1         ET TROJAN Backdoor family PCRAUChost Cnc Traffic (OUTBOUND) 106       2       1         ET TROJAN Davide ITTR/IN Describe Mind and a Text File       2       1         ET TROJAN Describe Mindicious SSL Cert (MageCart Cnc)       2       1         ET TROJAN Describe Mindicious SSL Cert (MageCart Cnc)       1       1         ET TROJAN Describe Mindicious SSL Cert (MageCart Cnc)       1       1         ET TROJAN Describe Mindicious SSL Cert (MageCart Cnc)       1       1         ET TROJAN Describe Mindicious	ET TROJAN Injected WP Keylogger/Coinminer Domain Detected (cloudflare .solutions in DNS Lookup)	10	1
FTPRO TROJAN Win32/Megalodon/AgentTesta Conn Check       1         ETPRO TROJAN Win32/Megalodon/AgentTesta Conn Check       6       1         ET TROJAN Self-Signed Cett Observed in Various Zbot Strains       6       1         ET TROJAN Double HTTP/11 Header Inbound - Likely Hostile Traffic       5       2         ET TROJAN Motor frainly PCRAtrikohost - Ch traffic       4       2         ET TROJAN Buckofor frainly PCRAtrikohost - Ch traffic       3       2         ET TROJAN Buckofor frainly PCRAtrikohost - Ch traffic       3       2         ET TROJAN Buckofor frainly PCRAtrikohost - Ch traffic       3       2         ET TROJAN Backdoor frainly PCRAtrikohost - Ch traffic (UtroBOUND) 106       2       1         ET TROJAN Backdoor frainly PCRAtrikohost - Ch traffic (UtroBOUND) 106       2       1         ET TROJAN Possible Windows executable sent when remote host claims to send a Text File       2       1         ET TROJAN Doserved Malicious SSL Cert Mag 12 2015       2       1       1         ET TROJAN Backdoor Win32 ZMShet Ping Outbound       1       1       1       1         ET TROJAN Backdoor Win32 ZMShet Ping Outbound       1       1       1       1         ET TROJAN Backdoor Win32 ZMShet Ping Outbound       1       1       1       1         ET TROJAN Backdoor Win32 ZMShet Ping O	ET TROJAN CobaltStrike DNS Beacon Response	9	1
ETPRO TRO JAN Win32/Megiadodn/AgentTesia Conn Check1ET TRO JAN Self-Signed Cart Observed In Various Zbot Strains52ET TRO JAN Double HTTP/11 Header Inbound - Likely Hostile Traffic72ET TRO JAN Bokedoor family PCRAt/Chost Ccr traffic42ET TRO JAN Self-Signed Cart Observed Microband (pugin)31ET TRO JAN Self-Signed Kart Observed Microband (pugin)31ET TRO JAN Self-Signed Kart Observed Microband (pugin)21ET TRO JAN Self-Signed Kart Operation Securitizate detected (Torrent.ocker CrC)21ET TRO JAN Self-Signed Kart Operation Securitizate detected (Torrent.ocker CrC)21ET TRO JAN Self-Signed Kart Operation Securitizate detected (Torrent.ocker CrC)21ET TRO JAN Self-Signed Kart Operation Securitization Securit	ET TROJAN Likely Bot Nick in IRC (Country Code ISO 3166-1 alpha-2	8	1
ET TROUAN Self-Sliped Cert Observed in Various Zbot Strains61ET TROUAN Self-Sliped Cert Observed in Various Zbot Strains52ET TROUAN Double HTTP/1.1 Header Inbound - Likely Hostile Traffic42ET TROUAN Backdoor family PCRat/Ghost Cnc traffic41ET TROUAN MSIL/Molf RAT Cnc Command Inbound (plugin)41ET TROUAN MSIL/Molf RAT Cnc Command Inbound (plugin)32ET TROUAN MSIL/Molf RAT Cnc Command Inbound (plugin)32ET TROUAN MSIL/Molf RAT Cnc Command Inbound (plugin)32ET TROUAN Self-CH SLi Blacklist Malicious SSL certificate detected (Torrent-Locker Cnc)21ET TROUAN Backdoor family PCRat/Ghost Cnc traffic (OUTBOUND) 10621ET TROUAN Self-CH SLi Blacklist Malicious SSL cert (Jug 12 201521ET TROUAN Possibie Dride's SSL Cert Aug 12 201521ET TROUAN Backdoor Xinia Z Shot Ping Outbound11ET TROUAN Backdoor Xinia Z Shot Ping Outbound11ET TROUAN Backdoor Xinia Z Shot Ping Outbound11ET TROUAN Subjelicous SSL Cert (MageCart Cnc)11ET TROUAN Subjelicous SSL Cert (MageCart Group 12)11ET TROUAN Sub	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1	8	1
TROJAN Double HTTP/11 Header Inbound - Likely Hostile Traffic       5       2         ET TROJAN Backdoor family PCRat/Gh0st Chc Ctraffic       4       1         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 Backdoor family PCRat/Gh0st Cnc traffic (OUTBOUND) 106       2       1         ET TROJAN Backdoor family PCRat/Gh0st Cnc traffic (OUTBOUND) 106       2       1         ET TROJAN Selection SSL Cert Aug 12 2015       2       1         ET TROJAN Possible Windows executable sent when remote host claims to send a Text File       2       1         ET TROJAN Selection SSL Cert Mug 2015       2       1       1         ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)       2       1       1         ET TROJAN Selection Wind/Selection SSL Cert (MageCart CnC)       2       1       1         ET TROJAN Nobserved Malicious SSL Cert (MageCart Group 12)       1       1       1       1         ET TROJAN Selection Selection Wind/Selection SSL Cert (MageCart Group 12)       1       1       1       1         ET TROJAN Netwire RAT Client HeartBeat       1       1       1       1       1       1       1       1       1       1	ETPRO TROJAN Win32/Megalodon/AgentTesla Conn Check	7	1
TROJAN Backdoor family PCRat/GN0bt Cht Taffic42ET TROJAN Backdoor family PCRat/GN0bt Cht Taffic32ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Torrent Locker CnC)21ET TROJAN Backdoor family PCRat/GN0bt CnC traffic (OUTBOUND) 10621ET TROJAN Backdoor family PCRat/GN0st CnC traffic (OUTBOUND) 10621ET TROJAN Spible Dridex SSL Cert Aug 12 201521ET TROJAN Possible Unidows executable sent when remote host claims to send a Text File21ET TROJAN Deserved Malicious SSL Cert (MageCart CnC)21ET TROJAN Deserved Malicious SSL Cert (MageCart CnC)11ET TROJAN Deserved Malicious SSL Cert (MageCart Group 12)11ET TROJAN Deserved Malicious SSL Cert (MageCart Group 12)11ET TROJAN Spipleious Download Stup_exe11ET TROJAN Windrow SWIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET ROJAN Malicious SSL Cert (MageCart Group 12)11ET ROJAN Malicious SSL Cert (MageCart CnC)11ET ROJAN Malicious SSL Cert (Mindows DOS prompt command exit OUTBOUND11ET ROJAN Malicious SSL Cert (Mindows Cort ChC)11ET ROJAN Malicious SSL Cert (Mindows ChC)11ET ROJAN Malicious SSL Cert (Mindows ChC)1	ET TROJAN Self-Signed Cert Observed in Various Zbot Strains	6	1
TROJAN MSIL/Modi RAT Ch Command Inbound (plugin)41ET TROJAN Possible Windows executable sent when remote host claims to send htmi content21ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)21ET TROJAN Backdoor family PCRat/Ghöst CnC traffic (OUTBOUND) 10621ET TROJAN Generic DNS Query for Suspicious CryptoWall (crpt) Domains21ET TROJAN Possible Dridex SSL Cert Aug 12 201521ET TROJAN Observed Malicious SSL Cert (MageCart CnC)21ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)21ET TROJAN Doserved Malicious SSL Cert (MageCart Group 12)11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN SUBJECUS Set Mindows WINC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET ROJAN Malicious SSL Certificate Detected (Gootkit C2)111ETRO TROJAN Malicious SSL Certificate Detected (Ursnif CnC)111ETRO TROJAN Malicious SSL Certificate detected (Ursnif CnC)1	ET TROJAN Double HTTP/1.1 Header Inbound - Likely Hostile Traffic	5	2
TROLAR Nossible Windows executable sent when remote host claims to send html content32ET TROJAN ABUSE.CH SSL Blackilst Malicious SSL certificate detected (TorrentLocker CnC)21ET TROJAN ABUSE.CH SSL Blackilst Malicious SSL certificate detected (TorrentLocker CnC)21ET TROJAN Generic DNS Query for Suspicious CryptoWall (cryt) Domains21ET TROJAN Possible Dridex SSL Cert Aug 12 201521ET TROJAN Possible Windows executable sent when remote host claims to send a Text File21ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)21ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)11ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)11ET TROJAN Doserved Malicious SSL Cert (MageCart Gnop 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windows WINC PROCESS get Microsoft Windows DOS prompt command ext OUTBOUND11ET TROJAN Malicious SSL Certificate Detected (Ocotkit C2)11ET ROJAN Malicious SSL Certificate Detected (Ursnif CnC)11ET ROJAN Malicious SSL Cert	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic	4	2
ET TRO JAN ABUSE.CH SL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)21ET TRO JAN Backdoor family PCRAt/Ghost CnC traffic (OUTBOUND) 10621ET TRO JAN Generic DNS Query for Suspicious CryptoWall (cryt) Domains21ET TRO JAN Possible Dridex SSL Cert Aug 12 201521ET TRO JAN Doserved Malicious SSL Cert (MageCart CnC)21ET TRO JAN Doserved Malicious SSL Cert (MageCart CnC)11ET TRO JAN Doserved Malicious SSL Cert (MageCart Group 12)11ET TRO JAN Doserved Malicious SSL Cert (MageCart Group 12)11ET TRO JAN Supicious Download Setup_ exe11ET TRO JAN Multichous SSL Cert (ficate Detected (Gootkit C2)11ET TRO JAN Malicious SSL Cert (ficate Detected (Gootkit C2)11ET RO TRO JAN Malicious SSL Cert (ficate Detected (Ursnif CnC)11ET ROT AND Malicious SSL Cert (ficate Detected (Gootkit C2)11ET ROT AND Malicious SSL Cert (ficate Detected (Ursnif CnC)11ET ROT AND Malicious SSL Cert (ficate Detected (Ursnif CnC)11ET ROT AND Malicious SSL Cert (ficate Detected (Ursnif CnC)11ET ROT AND Allicious SSL Cert (ficate Detected (Ursnif CnC)11ET ROT AND Allicious SSL Cert (Ficate Detected (Ursnif CnC)11ET ROT AND Allicious SSL Cert (Ficate Detected (Ursnif CnC)11ET ROT AND Allicious SSL Cert (Ficate Detected (Ursnif CnC)11ET ROT AND Allicious SSL Cert (Ficate Detected (Ursnif CnC)11 <td>ET TROJAN MSIL/Modi RAT CnC Command Inbound (plugin)</td> <td>4</td> <td>1</td>	ET TROJAN MSIL/Modi RAT CnC Command Inbound (plugin)	4	1
ET TROJAN Backdoor family PCRat/Gh0st Cnc traffic (OUTBOUND) 10621ET TROJAN Generic DNS Query for Suspicious CryptoWall (crpt) Domains21ET TROJAN Possible Dridex SSL Cert Aug 12 201521ET TROJAN Possible Windows executable sent when remote host claims to send a Text File21ET TROJAN Doserved Malicious SSL Cert (MageCart CnC)21ET TROJAN Backdoor Win32.RShot Ping Outbound111ET TROJAN Netwire RAT Client HeartBeat111ET TROJAN Doserved Malicious SSL Cert (MageCart Group 12)111ET TROJAN Suspicious Download Setup_exe1111ET TROJAN Mindrows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND1111ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)1111111ETPRO TROJAN Malicious SSL Certificate Meterded (Ursnif CnC)111 </td <td>ET TROJAN Possible Windows executable sent when remote host claims to send html content</td> <td>3</td> <td>2</td>	ET TROJAN Possible Windows executable sent when remote host claims to send html content	3	2
ET TROJAN Generic DNS Query for Suspicious CryptoWall (crpt) Domains21ET TROJAN Possible Dridex SSL Cert Aug 12 201521ET TROJAN Possible Windows executable sent when remote host claims to send a Text File21ETPRO TROJAN Observed Malicious SSL Cert (MageCart CnC)21ET TROJAN Backdoor.Win32.RShot Ping Outbound11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windrows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET ROJAN Malicious SSL Certificate Detected (Gortkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN Malicious SSL certificate Agecart Size11ETPRO TROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TorrentLocker CnC)	2	1
ET TROJAN Possible Dridex SSL Cert Aug 12 201521ET TROJAN Possible Windows executable sent when remote host claims to send a Text File21ET TROJAN Observed Malicious SSL Cert (MageCart CnC)21ET TROJAN Backdoor.Win32.RShot Ping Outbound11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Notserved Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ET TROJAN Malicious SSL certificate detected (Ursnif CnC)11ET ROJAN Malicious SSL certificate detected (Ursnif CnC)11ET ROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 106	2	1
ET TROJAN Possible Wind were mente host claims to send a Text File21ET TROJAN Observed Malicious SSL Cert (MageCart CnC)21ET TROJAN Backdoor.Win32.RShot Ping Outbound11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ET TROJAN Malicious SSL certificate detected (Ursnif CnC)11ET TROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN Generic DNS Query for Suspicious CryptoWall (crpt) Domains	2	1
ETPRO TROJAN Observed Malicious SSL Cert (MageCart CnC)21ET TROJAN Backdoor.Win32.RShot Ping Outbound11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET PRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ET PRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ET PRO TROJAN Tiny Loader.C nc Beacon x8611	ET TROJAN Possible Dridex SSL Cert Aug 12 2015	2	1
ET TROJAN Backdoor.Win32.RShot Ping Outbound11ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11	ET TROJAN Possible Windows executable sent when remote host claims to send a Text File	2	1
ET TROJAN Netwire RAT Client HeartBeat11ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)11ET TROJAN Suspicious Download Setup_ exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN Malicious SSL certificate Attences Malicious11ETPRO TROJAN Malicious SSL certificate Attences Malicious11ETPRO TROJAN Malicious SSL certificate Microsoft Windows Microsoft Windows11	ETPRO TROJAN Observed Malicious SSL Cert (MageCart CnC)	2	1
ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)1ET TROJAN Suspicious Download Setup_exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN Backdoor.Win32.RShot Ping Outbound	1	1
ET TROJAN Suspicious Download Setup_exe11ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN Netwire RAT Client HeartBeat	1	1
ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND11ET PRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)11ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)11ETPRO TROJAN TinyLoader.C CnC Beacon x8611	ET TROJAN Observed Malicious SSL Cert (MageCart Group 12)	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	ET TROJAN Suspicious Download Setup_ exe	1	1
ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)     1     1       ETPRO TROJAN TinyLoader.C CnC Beacon x86     1     1	ET TROJAN Windows WMIC PROCESS get Microsoft Windows DOS prompt command exit OUTBOUND	1	1
ETPRO TROJAN TinyLoader.C CnC Beacon x86	ETPRO TROJAN Malicious SSL Certificate Detected (Gootkit C2)	1	1
	ETPRO TROJAN Malicious SSL certificate detected (Ursnif CnC)	1	1
ETPRO TROJAN Win32/Quervar.C Possible NetBIOS Query (KASPERSKY) 1 1	ETPRO TROJAN TinyLoader.C CnC Beacon x86	1	1
	ETPRO TROJAN Win32/Quervar.C Possible NetBIOS Query (KASPERSKY)	1	1

### Exploit IoCs

loC description 🗢				Count ≑	Unique Org
ET EXPLOIT Multiple DrayTek Products P		• • •		344	4
ET EXPLOIT MVPower DVR Shell UCE	IoC description 🗢	Count ≑	Unique Orgs 🕯	178	3
ET EXPLOIT Zyxel NAS RCE Attempt Inbo	China	<b>QQ</b> 241	3	<b>QQ</b> 141	4
ET EXPLOIT Multiple DrayTek Products P	United States	214	8	119	3
ET EXPLOIT [401TRG] ZeroShell RCE Inb	Brazil	57	3	97	2
ET EXPLOIT Joomla RCE M3 (Serialized I	France	57	3	69	3
ET EXPLOIT Netgear DGN Remote Comn	Indonesia	43	2	69	2
GPL EXPLOIT Microsoft cmd.exe banner	Canada	40	2	56	1
ET EXPLOIT MS-SQL SQL Injection closir	Mexico	39	3	46	1
ET EXPLOIT HackingTrio UA (Hello, World	Russia	36	3	42	3
T EXPLOIT [NCC GROUP] Possible Blue				28	1
T EXPLOIT D-Link Devices Home Netwo	Germany	34	2	25	2
T EXPLOIT Apache Struts Possible OGN	United Arab Emirates	34	2	24	2
T WEB_SPECIFIC_APPS Horde 3.0.9-3.1	Italy	33	3	14	1
T EXPLOIT Apache Struts getWriter and	Colombia	31	3	13	2
T EXPLOIT Apache Struts memberAcce	Ecuador	26	2	13	2
T EXPLOIT Apache Struts memberAcce	Egypt	24	3	13	2
T EXPLOIT Possible TLS HeartBleed Un	South Korea	22	2	10	1
T EXPLOIT Mikrotik Winbox RCE Attemp	Azerbaijan	21	2	9	3
T EXPLOIT COMTREND ADSL Router C	Australia	18	3	6	3
T EXPLOIT D-Link Router DNS Changer		17		6	3
T EXPLOIT Generic ADSL Router DNS C	India		3	6	3
T EXPLOIT Possible ShuttleTech 915WN	Vietnam	16	2	6	3
GPL EXPLOIT ISAPI .ida access	Switzerland	15	1	6	2
GPL EXPLOIT iissamples access	Hong Kong	14	4	6	2
T EXPLOIT Linear eMerge E3 Unauthen	Netherlands	14	2	5	2
T EXPLOIT MVPower DVR Shell UCE MS	Panama	14	2	5	2
T EXPLOIT Possible OpenSSL HeartBlee	a Large HeartBeat Response from Common SSL Port (Outbound from Client)			5	1
T EXPLOIT SSL excessive fatal alerts (po	ssible POODLE attack against server)			5	1
T EXPLOIT D-Link DSL-2750B - OS Com	nand Injection			4	1
TPRO EXPLOIT Adobe Acrobat Reader A	CE.dll ICC mluc Integer Overflow			4	2

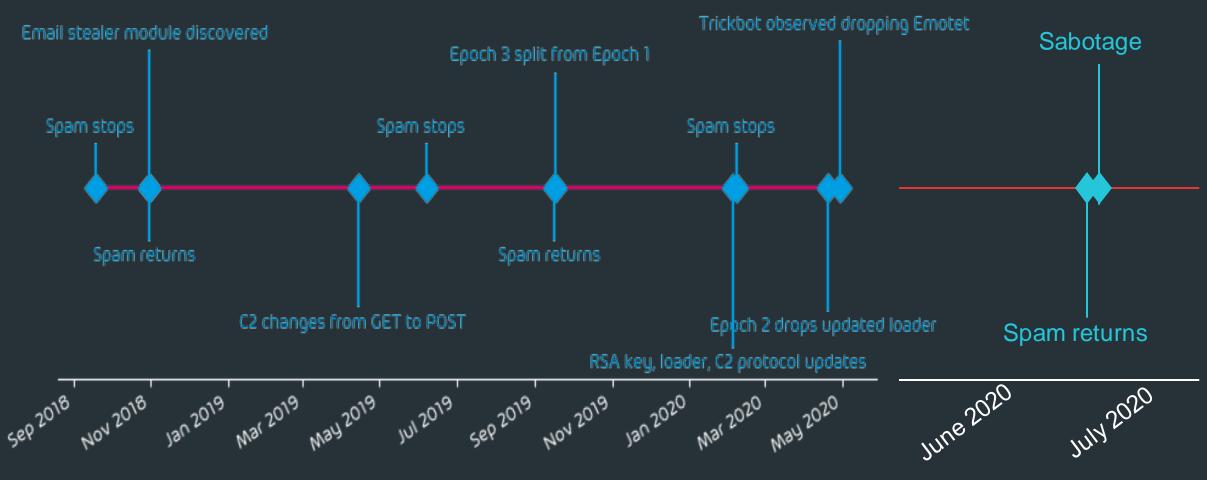


### Guess who's back?

## **Emotet**



## Recent Emotet Timeline





### Hack Back?



•

### Emotet -> Ryuk Ransomware





### **Ransomware Leaks**



Ransom Leaks -@ransomleaks

#REvil keeps serving up the breaches. Sanitary Process Engineering Components (SPEC) was hit with Sodinokibi ransomware.

No ransom was paid and now a leak is being threatened.

#### Keep your networks clean folks.

	t US SPEC Inc. www.saritzyprocess.com We have downloaded youry download link will be soon.
Engineering & Components, Inc.	Varia
> help customers meet their challenges by providing ts and services in a timely and cost effective manner.	PC + Shared C Name P. Devenue MCRANI 9: SPEC.Logo N: TackO
at. With a staff that has a combined 80- years of experience in There. All tasks and challenges are welcomed.	Plue Pomp SAGE INST SPEC INFO
	LC PROMU Searers Pa Searers Pa Company I MONTHSE CTIC Save DXION-BR
	Pointend 2009 Grids a AMPCO DM SCOULD Wab site at Process
	Contraction Contractions

ryprocess.com mixeded your private data, documents about customers and et k will be soon. Company lofa ESET 0/T Flux Fump SAGE INSTR SPEC INFO C D Postand 🗆 💼 Rutherg 🗆 🖿 John Marrall C Prong 1028/2019 11/28/201 🗇 📷 Sasawe Puny Detail 19/25/201 C . Brec mro

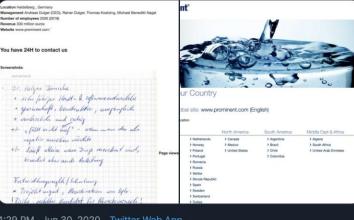
7:17 PM · Jun 17, 2020 · Twitter Web App



#CIOp #Ransomware crew claims ProMinent Fluid Controls as a victim.

CLOP threatens to leak data from the organization in 24 hours if they do not respond to negotiations.

#### ProMinent has 2100 employees and 450m revenue



4:29 PM · Jun 30, 2020 · Twitter Web App

8 Retweets and comments 3 Likes



#DoppelPaymer #ransomware team recently claimed Knoxville, TN as victim.

"City officials said [..] no financial or personal information had been accessed", but leaks show that's not true.

Hacked hosts include numerous Knoxville Police Department servers.

City of Knoxville TN:	DC+knowvilletn,DC+gov	DNSDHCP1-TEMP	Windows Server 2016 Standard	DNSDHCP1-TEMP.oly.knoxvilletn.gov
URL	DC=knoxvilletn,DC=gov	CAU4102019	Windows Server 2016 Standard	CAU4102019.city.knoxvilletn.gov
https://knoxvilletn.gov	willeth.DC-gov	CAU	Windows Server 2016 Standard	CAU.city:knoxvilletn.gov
Details	nosvilletn,DCgov	WIN2016VM	Windows Server 2016 Standard	Win2016VM.city.knowvilletin.gov
* though city officials said their initial assessment shows no financial or personal information had been compromised.*	knoxvilletn,DCgov	MATSON	Windows Server 2016 Standard	Watson city knowlitetn gov
Watch for updates.	nosvilletn.DC=gov	220FBROB	Windows Server 2016 Standard	FBRDB. city knowvillets.gov
	enoevilletri,DC=gov	222 FBRAPP	Windows Server 2016 Standard	FBRAPP.city.know/lietn.gov
Example files:	n.DC-gov	222	Windows Server 2016 Standard	aity knowlifetn.gov
New Iolaier, 72.053 (10240000) New Iolaier, 72.05 (10240000) New Iolaier, 72.05 (10240000) New Iolaier, 72.05 (10240000) New Iolaier, 72.05 (10240000)	enoevilletn.DC=gov	APPTESTOB	Windows Server 2016 Standard	AppTestDB.city.knoxvilletn.gov
	evilletn,DC~gov	KATFUEL	Windows Server 2016 Standard	KATFUEL city/know/lietn.gov
New folder.72.009 (102400Kb) New folder.72.059 (102400Kb)	villetn,DC=gov	FIFSAS1	Windows Server 2016 Standard	FIFSAS1.city knowlifetin.gov
New folder 72.000 (102400Kb) New folder 72.001 (102400Kb)	villetn,DCgov	FIFSAS2	Windows Server 2016 Standard	FIFSAS2.city knowlifetn.gov
New folder 72.003 (102400Kb) New folder 72.003 (102400Kb)	Retn.DCgov	FIMON	Windows Server 2016 Standard	FIMON.city knowvilletn.gov
New (older: 72.064 (102400Kb) New (older: 72.065 (102400Kb)	DC=knoxvilletn,DC+gov	MPS-FIRECOMM	Windows Server 2016 Standard	MPS-FireComm.oity:knosvilletn.gov
New (older:7z.066 (102400Kb) New (older:7z.067 (102400Kb)	C-knoxvilleth.DC+gov	MPS-2018COMM	Windows Server 2016 Standard	MPS-2022Comm.city knowvilletn.gov
New folder.7z.088 (102400Kb) New folder.7z.089 (102400Kb)	Ry.DC=knowilletn,DC=gzv	WIN-381ONL1RDTN	Windows Server 2016 Standard	WIN-381ONL1RDTN.city knowlitetn.gov
New folder.7z.070 (54511Kb) inf.7z.001 (102400Kb)	villetn,DC+gov	222 APP	Windows Server 2016 Standard	APP.city knowvilletn.gov

#### 10:53 AM · Jul 4, 2020 · Twitter Web App

8 Retweets and comments 8 Likes



### 2020 MSP https://go.perchsecurity.com/SR-2020 Threat Report as As we the th when ranso these acces Becau can d Ranso lucrat PERCH

### Sodinokibi

- Sodinokibi (aka Sodin or REvil) is offered by PINCHY SPIDER in a Ransomware-asa-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 Sodinokini 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

6.1%

### 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

2.8%

### 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

### CLOP

TA505 adopted Clop Ransomware as their final payload of choice after compromising a network," -<u>https://www.bleepingcomputer.com/news/security/clop-</u> <u>ransomware-now-kills-windows-10-apps-and-3rd-party-tools/</u>

TA505, the name given by Proofpoint, has been in the cybercrime business for at least four years. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet. Other malware associated with TA505 include Philadelphia and Globel mposter ransomware families.

"Looking at the Clop ransom note, it shares TTPs with other ransomware families; e.g. it mimics the Ryuk ransomware and contains similarities with BitPaymer, however the code and functions are quite different between them." – McAffee

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clopransomware/



MalwareHunterTeam @malwrhunterteam

Signed & low detected (as usual), yesterday evening build of CryptoMix Clop ransomware sample:

1

#### virustotal.com/en/file/2ceeed...

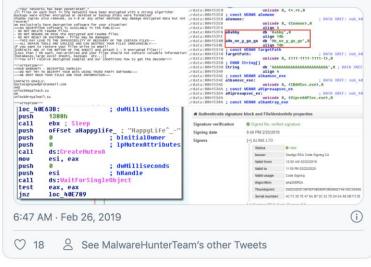
Again some changes in the note, and now it has 3 email addresses...

Also, new mutex and "messages" too.

#### ed arr

#### @demonslay335

cc @VK\_Intel





go.perchsecurity.com/share

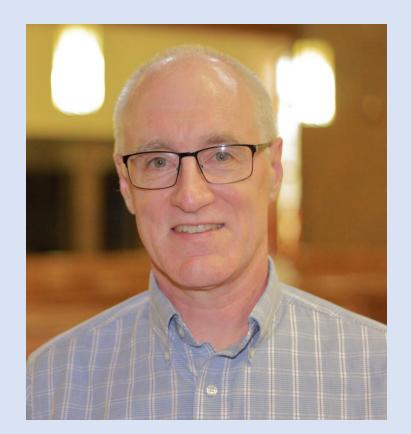
## A Member's Perspective

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 <u>CVE-2020-1425</u> and <u>CVE-2020-1457</u> and apply the necessary updated. <u>Read the advisory at CISA</u>.

## 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 <u>CVE-2020-1425</u> and <u>CVE-2020-1457</u> and apply the necessary updates. <u>*Read the advisory at CISA.*</u>

## Perch Threat Indicators are already in place

#### **Recent Indicators**

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



Red Created: July 7th 2020, 5:40:59 PM UTC Description: [Perch Security] PUP Activity - Suspicious Redirects

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



Created: July 7th 2020, 5:40:59 PM UTC Description: [Perch Security] Malware CAB File Drop

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

#### White

Red

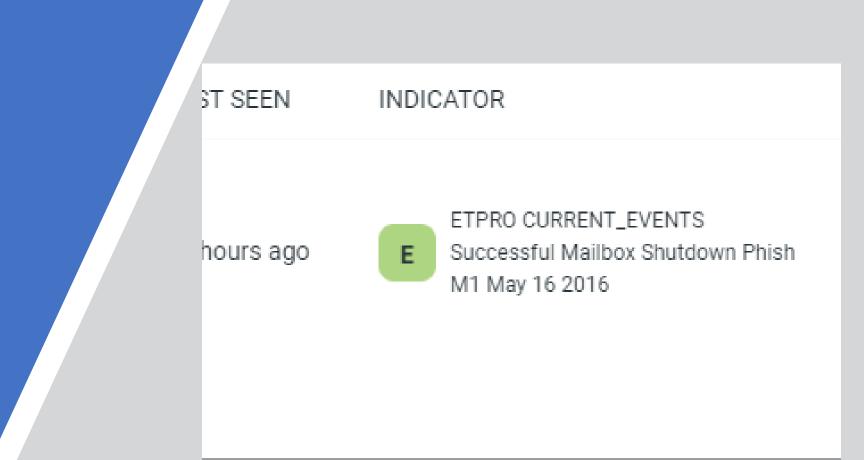
Created: July 7th 2020, 9:38:51 AM UTC Description: Australian Cyber Security Centre Indicators of Compromise Release

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



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.



## 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

(i) This notification uses data for OCWA. General	
OT Traffic Notification	±
Description Display an alert if traffic is detected between the OT Netwo	ork and the Internet

## 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.

# Want to try Perch?

Go.perchsecurity.com/share