ORDR SECURITY BULLETIN

Ryuk Ransomware Detection Using Ordr

Notices

This documentation and its content are subject to change without notice. Ordr and its licensors assume no responsibility or liability for any errors, inaccuracies, or omissions in this documentation. Nothing in this documentation should be construed as a commitment or warranty of any kind.

Content

Overview

Ransomware is one of the biggest threats to enterprises as seen by the recent attack on United Health Services (UHS), a health care organization with nearly 400 facilities in the U.S., U.K., and Puerto Rico. The following link provides details on this incident:

https://www.helpnetsecurity.com/2020/09/29/uhs-cyberattack/

Ryuk uses a couple of well-known trojans like Emotet and Trickbot for initial delivery, internal reconnaissance, command and control communication, credential harvesting, and other aspects of an Advanced Persistent Threat (APT) attack. This paper examines how Ordr can help detect, defend, and respond to these attack vectors employed by this APT attack.

RYUK Scenarios

Initial Delivery

Ryuk uses the Emotet Trojan as the initial weapon to gain access to the system. The Emotet Trojan downloader is sent as a Microsoft Word document (for example, as an invoice) attached via a phishing email, to make it seem legitimate and benign. When the document is opened, the user is tricked into enabling macros in the Word documents to view them. Doing so will launch the macros and launches the attack.

Execution and Persistence

The macros that are executed in the document will in turn launch PowerShell and download the Emotet payload from a remote host. Once Emotet executes, it also downloads Trickbot to do further reconnaissance.

Privilege Escalation

A recent addition to the Trickbot arsenal of modules is *rdpScanDll'* which allows the malware to brute-force Remote Desktop Protocol (RDP) credentials. Another mechanism employed by Trickbot is the creation of service user accounts once it has access to authentication servers in the network.

Defense Evasion

Trickbot employs several different techniques for obscurity and evasion. TLS is used for command and control (C2) communications and while downloading the various modules for installation. C2 typically happens on the standard TLS port 443 but has also been observed to use port 449. TLS is not the only form of encryption used by Trickbot. While withdrawing sensitive information from a compromised host, the Microsoft CryptoAPI is used to encrypt the data as an extra layer of obscurity.

Discovery and Credential Access

Trickbot uses the following techniques to gain user credentials and network topology:

- *InjectDll* module to steal credentials by using *Webinjects* on websites.
- *MailSearcher* module to search documents and images for sensitive information.
- *SystemInfo* module to enumerate the system information on the infected host.

Lateral Movement

There are several exploit techniques used by Trickbot for lateral movement including EternalBlue and EternalRomance – these techniques allow the malware to spread within the enterprise network so the threat actors can get close to the intended sensitive assets/information.

Trickbot also uses *shareDll32* and *shareDll64* modules that leverage SMB shares to transfer a copy of the Trickbot trojan to any administrative servers in the network.

Collection

With the credentials, network information and sensitive servers learned so far, the threat actors use RDP sessions to gain access to the key servers and perform further actions such as encryption.

Command and Control

Threat Actors control the infected system remotely using a reverse shell that is part of the Trickbot trojan. This C&C channel allows them to download additional payloads and scripts and navigate the systems in the network.

Exfiltration

PSEXEC is used to push out the Ryuk binary to individual hosts. Batch scripts are executed to terminate processes/services and remove backups, followed by the Ryuk binary.

ATT&CK Framework / Ordr Capabilities

This table shows the activities that are present at the various stages of an attack. The Ordr Systems Control Engine (SCE) detects these activities individually through its various data collection and ingestion channels.

Some infection stages in the table are addressed by tools more appropriate for that category of activity but are included for completeness. Ordr's visibility and anomaly detection provides broad coverage to help in this area.

Infection Stage	Network and Device Activity
Reconnaissance	
Resource Development	
Initial Access	External Remote Services
	Hardware Additions
	Phishing
Execution	System Services
	Windows Management Instrumentation
Persistence	External Remote Services
	Valid Accounts
Privilege Escalation	
Defense Evasion	
Credential Access	Man-in-the-Middle
	Unsecured Credentials
Discovery	Account Discovery
	Network Share Discovery
	Password Policy Discovery
	Peripheral Device Discovery
	Permission Groups Discovery
	Remote System Discovery
	System Information Discovery
	System Network Configuration Discovery
	System Network Connections Discovery
Lateral Movement	Exploitation of Remote Services
	Internal Spearphishing
	Lateral Tool Transfer

Infection Stage	Network and Device Activity
	Remote Service Session Hijacking
	Remote Services
Collection	Archive Collected Data
	Data from Network Shared Drive
	Main-in-the-middle
Command and Control	Application Layer Protocol
	Communication Through Removable Media
	Data Encoding
	Data Obfuscation
	Dynamic Resolution
	Encrypted Channel
	Fallback Channels
	Ingress Tool Transfer
	Multi-Stage Channels
	Non-Application Layer Protocol
	Non-Standard Port
	Protocol Tunneling
	Proxy
	Remote Access Software
	Traffic Signaling
	Web Service
Exfiltration	Automated Exfiltration
	Data Transfer Size Limits
	Exfiltration Over Alternative Protocol
	Exfiltration Over C2 Channel
	Scheduled Transfer
Impact	Account Access Removal
	Endpoint Denial of Service

The color codes used in this table are detailed in the following legend which assigns a color to each detection capability. Refer to the following text by the Index number for further explanation.

Index/Color Code	Detection
1	AD-based checking on valid accounts reporting

2	Internal movement monitoring – IDS rules
3	Behavior-Based line-based anomaly detection
7	Ext Conn Monitoring – Connection to C&C channels
8	Ordr Discovery
9	Packet statistics
10	Password checker and passwords on wire
11	RDP, SMB v1/v2 tracking

1. Active Directory (AD) based checking on valid accounts reporting

    - Ordr uses AD PowerShell to constantly pull all locally created user accounts, with special focus on the ones that house mission-critical functions. For example, healthcare PACS servers, where all patient images or PACS radiology data are stored, are one of the most critical systems in healthcare operations. If this system is locked by ransomware, a hospital cannot function.

    - Ordr collects and reports user login/logout activity in a form that can be analyzed to track the creation and usage of "fake user" accounts across a set of devices within the enterprise. Details such as timestamps are included. The data can be used for both real-time monitoring and forensic analysis.

      Ordr collects profiles on all users that have access to various machines and controls the access level to the minimum level required. A log of the access details (users, systems, duration) using the MSFT Active Directory is saved in the Ordr tool. Ordr also tracks all the wireless authentication activities to track how guest users are getting on to the system and accessing corporate applications.

2. Internal movement monitoring - IDS rules + behavior baseline

    - While Ordr tracks and maintains all communications, we can check for communication on abnormal ports like 449 to an external site and flag this as an error.

    - Ordr's IDS engine can detect certain signatures specific to Emotet and Trickbot in the SSL headers of the HTTPS communication with the C&C server.

    - Ordr detects all network reconnaissance operations (port scans and port sweeps) done by all the systems.

- Ordr uses intrusion detection engines that detect common Windows exploit mechanisms like EternalBlue, EternalRomance, etc., and provide an alert immediately when such an exploit is used.

- Additionally, Ordr's IDS engine has a specific signature that tracks Trickbot and Emotet trojans when they communicate on SMB port (like 445) for reconnaissance.

3. Behavior baseline and anomaly detection

   - Ordr profiles and baselines device communications and compares it with machines with similar functionality. If there are deviations in the baseline, Ordr highlights those unusual or suspicious communications as an alarm in its dashboard.

4. External Communications Monitoring - Connection to C&C channels

   - Ordr tracks all external URL connections especially from medical servers/workstations that house critical functions like CT-Scanners where images are hosted or collected.

   - The Ordr platform includes subscriptions to WebRoot and Firehole, industry-leading reputation checkers to constantly track this activity.

   - Ordr also can detect C&C sites/IPs and blacklist them.

5. Ordr Discovery

   - It is important to identify critical infrastructure devices and with what other devices it co-exists with. Accurate device profiling is key to not mix up critical infrastructure devices with devices that can freely roam the internet. Ordr has a tremendous set of capabilities to discover connected devices, classify them accurately with all its attributes like OS, make, model, manufacturer, patch levels, serial numbers, and other known characteristic attributes.

6. Packet Statistics

- Ordr tracks large data transfers. This type of activity is detected based on a device's deviation from a known baseline.
- External C&C and exfiltration sites can be detected by tracking FTP and other large data transfer protocols; for example, by monitoring the number of flows/bytes within a period to suspicious sites.

7. Ordr scanner and password checker
    - Ordr includes a built-in scanner to detect and track open IP ports.
    - Ordr includes a password scanner that detects default or weak passwords.

8. RDP, SMB v1/v2 tracking
    - The Ordr console can efficiently pull up a list of all machines that use this protocol RDP (port 3389) and SMBoTCP (port 445) and quickly assess if these services are needed on those machines.
    - Similarly, Ordr can track all SMBv1 and, SMBv2 activities, the devices associated with it, and remove this service from all the devices where it is not needed.
    - If RDP is needed, ensure that it comes in with SSH/IPsec tunnels with keys.
    - Also, if suspicious RDP activity is seen, then Ordr can be used to immediately obtain a list of machines that the infected devices is communicating with to chase down and identify any infections.

Ordr Best Practices

1. Track all outbound connections especially from medical devices where critical patient information is stored.
    - Ordr has a tracking system that correlates every outbound web connection with the URP/IP reputation of the site it is accessing. Ordr can then raise an

alarm when suspicious sites start communicating with devices inside the enterprise.

2. Identify Internal lateral movement to contain infection spreading.

    - Ordr has an intrusion detection system to identify all unnecessary lateral movement (for example - EternalBlue malware using signatures) within a VLAN/SUBNET and identifies all extraneous flows based on baseline deviation analysis for each device.

    - Ordr's automated micro-segmentation policies can be created and enforced to only allow sanctioned communications

    - Ordr can generate Access Control Lists (ACLs) to prevent internal lateral movement using switch ACLs. The following is a sample that Ordr can automatically generate and push to all the switches over SSH using Ordr's console.

      ```
      ip device tracking
      ip access-list extended ryuk-acl
      deny  udp any any eq 3389
      deny tcp any any eq 3389
      permit ip any any
      int gigabitethernet 2/3/1
      ip access group ryuk-acl in
      ```

    - Ordr pushes the generated ACLs only to specific Network Devices where they are required. The updates occur on devices where the infection is identified. This avoids performing network-wide rules updates that can cause network disruptions, and provides the fastest method to slow or stop the spread of the infection.

Ordr detects all intra-network reconnaissance attempts using its IDS and Flow Genome analysis technology. If a machine makes connection attempts to a number of machines within its VLAN/SUBNET that exceeds its usual patterns, Ordr identifies those anomalies and raises an alarm.

3. Restrict usage of vulnerable protocols.

    - Ordr can provide a complete list of all devices that use weak protocols like RDP(3389), SMBoTCP(445), and other supervisory protocols like SSH, Telnet, SCP, FTP, etc., If needed, Ordrcan provide granular details on all transactions of infected devices.

- Medical devices need maintenance access from manufacturers and the pathways opened for this purpose could be easily exploited by the malware. Ordr's baselining watches for external connections to understand and alarm on deviations.

4. Track the volume of network activity – both internal and external destinations.
   - Ordr provides a complete statistical analysis of the number of flows and volume of data transferred between various device groups, VLANs, Subnets, and other business level groups.
5. Quick action to contain the blast radius and microsegment to prevent malware spread.
   - Ordr provides automated actions to quickly address infections,
     I. shutting the port of the device.
     II. blacklisting the MAC address of the device.
     III. assigning devices to a quarantined VLAN.
   - Ordr also provides automated generation of access control lists to prevent protocols like RDP and SMB from spreading within a VLAN or subnet or among diverse business groups.

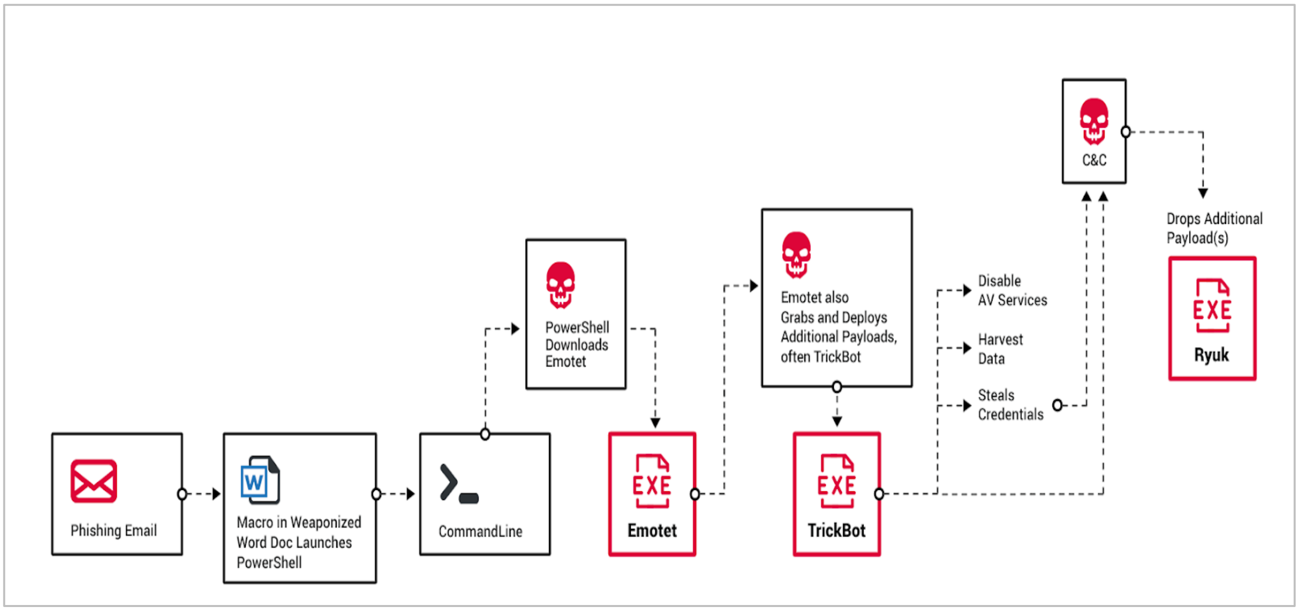
6. Make sure antivirus (AV) software is installed on all machines that can support security agents.
   - Ordr can continuously poll windows-based devices and collect an inventory of software packages installed to check for the presence of AV software.
   - Ordr can also track AV updates from devices to "AV update web sites" or internal servers to make sure the AV software is functioning and has not been disabled.
7. Get a complete inventory of hardware/software installed in all windows machines – especially the ones used for medical purposes.
8. Track user logon/logoff activity.
   - Ordr provides a mechanism to pull user logon activities from AD and track locally created users. This is very critical for machines like PACS servers where all the medical records are housed.

Appendix

Ryuk Attack Chain

Ryuk has been known to be a part of a bigger '*Triple Threat*' attack that involves Emotet and TrickBot.

- The first stage of this attack is the delivery of Emotet through phishing emails that contain a weaponized word document. This document contains a macro code that downloads Emotet.
- Once Emotet executes, it downloads another malware (usually TrickBot) which can collect system information, steal credentials, disable AV, perform a lateral movement.
- The third stage of the attack is to connect to the C&C server to download Ryuk, which makes use of the lateral movement by TrickBot to infect and encrypt as many systems on the network as possible.


Phishing Email
Macro in Weaponized Word Doc Launches PowerShell
CommandLine
PowerShell Downloads Emotet
EXE
Emotet
Emotet also Grabs and Deploys Additional Payloads, often TrickBot
EXE
TrickBot
Disable AV Services
Harvest Data
Steals Credentials
C&C
Drops Additional Payload(s)
EXE
Ryuk

Ref: https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/

Emotet

Emotet is often referred to as a banking trojan or worm. It is a very advanced threat that is updated multiple times a day by the cybercriminals controlling it. It has three primary goals:

- Spread onto as many machines as possible.
- Send malicious emails to infect other organizations.
- Download and execute a malware payload.

Traditionally, the payloads have mostly been banking Trojans, with TrickBot being the most prevalent. Other payloads have included Qbot, Dridex, or IcedID. There is also a connection between Emotet and a very dangerous targeted ransomware family called BitPaymer.

In July 2018, the U.S. Department of Homeland Security said the following in an alert:

"Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Additionally, Emotet is a polymorphic banking Trojan that can evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys and services. It uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine-aware and can generate false indicators if run in a virtual environment."

TrickBot

Like Emotet, TrickBot is also referred to as a banking trojan and worm. It performs a lot of similar activities as Emotet, for example, constantly trying to spread to other computers and updating itself multiple times a day. Its primary goal is to steal money by accessing users' online banking and PayPal accounts. TrickBot is arguably more advanced than Emotet as it has additional techniques it uses to spread, for example:

- Brute forcing usernames and passwords.
- Credential harvesting (taking usernames or passwords from memory when users log in).
- Using the vulnerability in Microsoft SMB known as EternalBlue (the same method that WannaCry ransomware used to spread).

- In addition, TrickBot is modular, meaning the attackers can pick and choose which type of attack they want to do.

In September 2018, the UK's National Cyber Security Centre published the following advisory:

"Trickbot is reported to have a range of malicious capabilities, including the ability to:

- Steal sensitive information, including banking login details and memorable information, by manipulating web-browsing sessions.
- Gather detailed information about infected devices and networks.
- Steal saved online account passwords, cookies, and web history.
- Steal login credentials for infected devices.
- Connect infected devices to malicious and criminally controlled networks over the Internet.
- Spread by infecting other devices on the victim's network.
- Download further malicious files such as Remote Access Tools, VNC clients, or ransomware".

Below are some of the Emotet infection with Trickbot.

Emotet-infection-with-Trickbot-in-AD-environment

Infected Packet Payload and the marked Signature of malware:

```
16 03 01 00 59 02 00 00 55 03 01 B1 2D C6 AA 69  ....Y...U...-..i
C7 1D 4C 1B FD FC 3E 0C 6C 56 C4 A8 6A A7 67 64  ..L...>.lV..j.gd
37 7E 68 27 F8 99 11 E2 7B E9 18 20 B2 AF 80 6F  7~h'....{.. ...o
2D 5A 3C 9E 8D 79 B6 D8 F9 C4 53 7E 3A B3 05 C2  -Z<..y....S~:...
43 9C 8D 60 7A 70 9A 4D 9E 3C A6 12 C0 14 00 00  C..`zp.M.<......
0D FF 01 00 01 00 00 0B 00 04 03 00 01 02 16 03  ................
01 03 6E 0B 00 03 6A 00 03 67 00 03 64 30 82 03  ..n...j..g..d0..
60 30 82 02 48 A0 03 02 01 02 02 09 00 E8 E1 72  `0..H..........r
64 7C 68 7D 5B 30 0D 06 09 2A 86 48 86 F7 0D 01  d|h}[0...*.H....
01 0B 05 00 30 45 31 0B 30 09 06 03 55 04 06 13  ....0E1.0...U...
02 41 55 31 13 30 11 06 03 55 04 08 0C 0A 53 6F  .AU1.0...U....So
```

```
6D 65 2D 53 74 61 74 65 31 21 30 1F 06 03 55 04  me-State1!0...U.
0A 0C 18 49 6E 74 65 72 6E 65 74 20 57 69 64 67  ...Internet Widg
69 74 73 20 50 74 79 20 4C 74 64 30 1E 17 0D 31  its Pty Ltd0...1
39 30 37 32 33 31 30 33 32 33 39 5A 17 0D 32 30  90723103239Z..20
30 37 32 32 31 30 33 32 33 39 5A 30 45 31 0B 30  0722103239Z0E1.0
09 06 03 55 04 06 13 02 41 55 31 13 30 11 06 03  ...U....AU1.0...
55 04 08 0C 0A 53 6F 6D 65 2D 53 74 61 74 65 31  U....Some-State1
21 30 1F 06 03 55 04 0A 0C 18 49 6E 74 65 72 6E  !0...U....Intern
65 74 20 57 69 64 67 69 74 73 20 50 74 79 20 4C  et Widgits Pty L
74 64 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D  td0.."0...*.H...
01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82  ..........0.....
01 01 00 D9 C5 98 C6 4D 43 0F A7 D2 91 FB DD 75  .......MC......u
30 35 4F 6E 70 23 21 6C D1 4C B5 32 35 D8 89 0A  05Onp#!l.L.25...
29 1C 44 3D 93 39 C1 F4 ED FF 87 00 2D A6 28 57  ).D=.9......-.(W
1E 25 FE 79 BC 1C FB 93 E4 02 AF 17 8F A4 79 D3  .%.y..........y.
82 80 67 63 9C 78 B8 16 0C D8 86 F6 F9 45 4C 93  ..gc.x.......EL.
2F 02 28 D0 A9 56 9D A7 08 FA 1C B2 F2 E8 83 D1  /.(..V..........
E9 AA 35 84 89 57 ED 5C 09 A3 E0 7B A4 51 8A C0  ..5..W.\...{.Q..
CC 06 FF 9C B7 B4 AB BB C1 A7 AF CD 72 00 67 99  ............r.g.
D9 F2 A5 FA C3 24 BC EC FE 60 58 A1 E6 55 BD 5E  .....$...`X..U.^
8D 10 9A B1 34 97 14 8C 11 2F 2A EC 06 85 DD DA  ....4..../*.....
69 0D 30 0F A6 17 80 20 20 5E A8 13 B4 33 1B E7  i.0....  ^...3..
66 70 DC 21 76 2F 01 D0 8F 27 0B FD 8B A1 0E 09  fp.!v/...'......
28 EC FE D7 BB AB 9B 74 E7 47 59 F5 14 5F FF 39  (......t.GY.._.9
34 AD CB 86 FB 68 90 E0 96 78 E2 AF 18 74 67 8E  4....h...x...tg.
CC EE E2 44 54 86 58 FB 6C E0 F8 60 05 9F 19 7F  ...DT.X.l..`....
B7 70 BE 22 74 44 22 BB EE 44 8B DB 6F 5B 40 70  .p."tD"..D..o[@p
CD F3 FF 02 03 01 00 01 A3 53 30 51 30 1D 06 03  .........S0Q0...
55 1D 0E 04 16 04 14 3E 24 C7 E3 9D 00 34 BE 74  U......>$....4.t
A1 12 C9 DD F1 BE 29 C1 EE C8 7C 30 1F 06 03 55  ......)...|0...U
1D 23 04 18 30 16 80 14 3E 24 C7 E3 9D 00 34 BE  .#..0...>$....4.
74 A1 12 C9 DD F1 BE 29 C1 EE C8 7C 30 0F 06 03  t......)...|0...
55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0D 06  U.......0....0..
09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82 01 01  .*.H............
00 B2 3C 02 67 EF B0 6A 9A AE 18 19 E6 F6 47 9A  ..<.g..j......G.
CA 33 44 A1 8B 35 BC 5E 0D 73 53 85 23 F0 7C FF  .3D..5.^.sS.#.|.
E1 FA 41 21 A8 A5 BB 72 19 E8 A3 53 16 29 94 4D  ..A!...r...S.).M
A1 A5 FA 2D 7E 6D 2F 2F E5 CC BD D9 1E 66 A7 B1  ...-~m//.....f..
73 74 54 04 D7 9B 68 DF 32 60 CA 4F D1 83 EF D3  stT...h.2`.O....
2E D1 28 58 18 4E C0 A6 0F 85 B6 35 07 EE D8 13  ..(X.N.....5....
C1 EA D7 53 F1 B2 0F 7A 4A 8C 3C C3 8A 34 B1 93  ...S...zJ.<..4..
31 3C AC 92 E2 6B 1E B4 72 2A F9 56 48 C4 88 03  1<...k..r*.VH...
5A 9B BB DB 03 E0 7E 95 C1 2E B5 A4 9B 4E 36 DF  Z.....~......N6.
C8 10 FA 61 5D 11 10 69 56 E0 B7 48 97 37 55 EA  ...a]..iV..H.7U.
DA 8A 7A 03 70 BD EF 5E 0C 89 20 31 21 F8 15 DF  ..z.p..^.. 1!...
13 3E 89 BF 6E 1A 32 F9 1D A0 DB C1 6F AD 6B C9  .>..n.2.....o.k.
EA 83 F2 C8 47 EF EF A3 1D 60 C2 CC C7 2E A2 CB  ....G....`......
```

```
6C 8F 9F 76 37 36 C5 8F 41 B0 B2 1B F4 C9 E1 01  l..v76..A.......
C3 8B CE 19 6C 5D 4B 6A 75 8B 70 EA 35 C8 8B 6B  ....l]Kju.p.5..k
B5 BF E4 49 FB 79 C0 13 14 EA 4C D4 ED 9C 8F 4F  ...I.y....L....O
3C 16 03 01 01 4B 0C 00 01 47 03 00 17 41 04 AF  <....K...G...A..
43 C2 82 39 05 A4 20 00 20 06 EF BD 64 4B C8 93  C..9.. . ...dK..
87 27 EB 4C 92 0A 45 0B 8C 10 E8 08 6A E9 D9 79  .'.L..E.....j..y
07 0C 49 77 C0 8A D7 79 A5 64 CA FD E4 F9 CB 7C  ..Iw...y.d.....|
33 95 FC A1 D7 A9 7C 08 DD F2 4E 08 32 6C 3D 01  3.....|...N.2l=.
00 1A 75 DE 83 1A A3 E8 9F 79 86 65 5C 3B 2D DA  ..u......y.e\;-.
0F 05 6D 27 9B 49 AE 09 31 1B A5 A2 51 40 76 F2  ..m'.I..1...Q@v.
A8 0D 37 4D CC A5 40 97 81 9F B5 B5 E3 B0 41 C0  ..7M..@.......A.
D9 1C 7A 64 08 03 8E 62 77 DA 99 16 5F C0 F4 A9  ..zd...bw..._...
AA DB C8 F6 34 FF 0A 0D A0 B2 9D 91 FB 6D A2 ED  ....4........m..
25 66 17 98 E8 6A C2 96 1D 53 01 9E A3 9D 22 51  %f...j...S...."Q
0F 60 32 1F 84 05 33 6A 92 B1 B1 09 8C 75 63 78  .`2...3j.....ucx
2B 50 98 A8 B6 7E 5C 5C 4A 7B D6 03 1D 8D FC 2B  +P...~\\J{.....+
E3 C3 35 D8 52 09 3E BA F1 E1 C6 CB 4D 68 3F 9F  ..5.R.>.....Mh?.
13 A4 8D 97 F5 C7 47 EE E5 89 D0 6F 4E DD 9B 19  ......G....oN...
96 94 8D 7E B0 01 4C DB 08 A6 F4 C6 5F 3E 7B EC  ...~..L....._>{.
56 DD 0A FD 1B BB C5 38 22 BB 07 71 2A 98 7A 66  V......8"..q*.zf
0D 24 D1 E5 B8 28 8A 90 8F FA 47 53 45 23 B1 89  .$...(....GSE#..
C3 33 1A 30 7C 09 DB DB 9E AC 2A F1 72 7C 00 C9  .3.0|.....*.r|..
F5 83 E0 92 40 74 CE 1B 51 33 01 C6 27 1C 20 BA  ....@t..Q3..'. .
15 ED A9 4F 6E 68 86 04 1B 78 D3 5F 59 D5 B8 D4  ...Onh...x._Y...
4F 16 03 01 00 04 0E 00 00 00                    O.........
```

IDS Rules Detection mechanism:

```
alert tcp $EXTERNAL_NET ![443,25,587] -> $HOME_NET any (msg:"ETPRO TROJAN
Observed Trickbot Style SSL Cert (Internet Widgets Pty Ltd)"; flow:established,from_server;
content:"|16|"; content:"|0b|"; within:8; content:"|06 03 55 04 06 13 02|AU"; distance:0;
content:"|06 03 55 04 08 0c 0a|Some-State"; distance:0; fast_pattern; content:"|06 03 55 04
0a 0c 18|Internet Widgits Pty Ltd"; distance:0; content:"|06 03 55 1d 13 01 01 ff 04 05 30
03 01 01 ff|"; distance:0; content:!"|06 03 55 04 06|"; distance:0; metadata:
former_category TROJAN; reference:md5,aabae4dd0effd2cd5875791e519bc576;
classtype:trojan-activity; sid:2837550; rev:3; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment
Perimeter, tag Trickbot, signature_severity Major, created_at 2019_07_16, malware_family
TrickBot, performance_impact Low, updated_at 2019_09_28;)
```

Emotet-epoch-2-with-Trickbot

Infected Payload and marked signature

```
16 03 03 00 50 02 00 00 4C 03 03 DA 9E E4 B3 80  ....P...L.......
57 AB 1A 88 47 73 F4 F8 DC C8 2B 9A 7B FD FD 53  W...Gs....+.{..S
9A 56 A4 DB DC C3 A3 A7 10 B1 41 00 C0 30 00 00  .V........A..0..
24 FF 01 00 01 00 00 0B 00 04 03 00 01 02 00 23  $..............#
00 00 00 17 00 00 00 10 00 0B 00 09 08 68 74 74  .............htt
70 2F 31 2E 31 16 03 03 03 D2 0B 00 03 CE 00 03  p/1.1..........
CB 00 03 C8 30 82 03 C4 30 82 02 AC A0 03 02 01  ....0...0.......
02 02 09 00 E2 08 FF FB 7B 53 76 3D 30 0D 06 09  ........{Sv=0...
2A 86 48 86 F7 0D 01 01 0B 05 00 30 77 31 0B 30  *.H.........0w1.0
09 06 03 55 04 06 13 02 47 42 31 0F 30 0D 06 03  ...U....GB1.0...
55 04 08 0C 06 4C 6F 6E 64 6F 6E 31 0F 30 0D 06  U....London1.0..
03 55 04 07 0C 06 4C 6F 6E 64 6F 6E 31 18 30 16  .U....London1.0.
06 03 55 04 0A 0C 0F 47 6C 6F 62 61 6C 20 53 65  ..U....Global Se
63 75 72 69 74 79 31 16 30 14 06 03 55 04 0B 0C  curity1.0...U...
0D 49 54 20 44 65 70 61 72 74 6D 65 6E 74 31 14  .IT Department1.
30 12 06 03 55 04 03 0C 0B 65 78 61 6D 70 6C 65  0...U....example
2E 63 6F 6D 30 1E 17 0D 32 30 30 32 30 33 32 30  .com0...20020320
30 36 30 30 5A 17 0D 32 31 30 32 30 32 32 30 30  0600Z..210202200
36 30 30 5A 30 77 31 0B 30 09 06 03 55 04 06 13  600Z0w1.0...U...
02 47 42 31 0F 30 0D 06 03 55 04 08 0C 06 4C 6F  .GB1.0...U....Lo
6E 64 6F 6E 31 0F 30 0D 06 03 55 04 07 0C 06 4C  ndon1.0...U....L
6F 6E 64 6F 6E 31 18 30 16 06 03 55 04 0A 0C 0F  ondon1.0...U....
47 6C 6F 62 61 6C 20 53 65 63 75 72 69 74 79 31  Global Security1
16 30 14 06 03 55 04 0B 0C 0D 49 54 20 44 65 70  .0...U....IT Dep
61 72 74 6D 65 6E 74 31 14 30 12 06 03 55 04 03  artment1.0...U..
0C 0B 65 78 61 6D 70 6C 65 2E 63 6F 6D 30 82 01  ..example.com0..
22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00  "0...*.H........
03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 B2 3C  .....0.........<
AD 04 91 E3 02 DC 73 00 60 77 A5 D6 DC 6F 77 EE  ......s.`w...ow.
80 20 C6 2C 96 14 03 F5 45 49 A9 E8 0A 10 84 B7  . .,....EI......
45 9B 3C 85 75 C4 9E 18 79 1F D6 FB 02 C2 34 5E  E.<.u...y.....4^
```

```
33 EA 28 75 95 DA 83 2A 53 28 B8 7E E6 4E A5 24  3.(u...*S(.~.N.$
36 88 CB 05 C8 BB 2F 91 C4 C2 A3 F2 39 BA 81 75  6...../.....9..u
1C 4F 1F BA F7 48 5E CE F5 BD AE BE 6F F1 E5 E6  .O...H^.....o...
9C F0 1C D7 39 D2 E2 CB FD C9 D3 AE BC A5 A2 2E  ....9..........
DF AC 4D 29 1D 06 BB 1B 85 FF B2 B0 BB CE 6E B7  ..M).........n.
37 C6 0C C7 D5 42 4F 8F 48 73 38 39 38 FC AD 85  7....BO.Hs898...
20 44 B4 D7 A4 44 1D 48 6A 83 FA A4 9D 04 72 0B   D...D.Hj.....r.
5B 40 15 41 05 A0 3F C7 99 F7 4A 34 ED 3A 13 7F  [@.A..?...J4.:..
0E B1 C9 96 CA 62 BC B7 3B F7 A9 B5 BD C6 94 BC  .....b..;.......
C4 4F F3 5F 43 B3 95 32 BE 25 6E 73 C3 9A 4E 0B  .O._C..2.%ns..N.
19 11 0D C9 99 EA CE E0 5F 72 3D E3 35 90 39 F2  ........_r=.5.9.
0F 49 D0 59 AE 6A 51 90 43 B1 8E A9 B6 E1 09 87  .I.Y.jQ.C.......
4F ED 3E AA 05 A1 12 EF 48 15 E3 7D 35 65 02 03  O.>.....H..}5e..
01 00 01 A3 53 30 51 30 1D 06 03 55 1D 0E 04 16  ....S0Q0...U....
04 14 B7 60 9B 13 9A 47 26 7A 1F 81 2B 7A B1 B1  ...`...G&z..+z..
72 32 72 69 DF 40 30 1F 06 03 55 1D 23 04 18 30  r2ri.@0...U.#..0
16 80 14 B7 60 9B 13 9A 47 26 7A 1F 81 2B 7A B1  ....`...G&z..+z.
B1 72 32 72 69 DF 40 30 0F 06 03 55 1D 13 01 01  .r2ri.@0...U....
FF 04 05 30 03 01 01 FF 30 0D 06 09 2A 86 48 86  ...0....0...*.H.
F7 0D 01 01 0B 05 00 03 82 01 01 00 84 70 C5 AF  ............p..
7F 76 F0 C1 07 19 8E 7F 94 09 08 27 B7 77 9C 54  .v.........'.w.T
BA A7 92 FE 29 3F 2D 59 FF 08 58 41 D4 7F E7 ED  ....)?-Y..XA....
C7 72 D7 49 A5 D4 BE 54 9A 9D E2 9C BF 3A A2 ED  .r.I...T.....:..
B2 5F 03 13 F1 6B 2C 28 0C 55 6A F9 96 E6 9A 3E  ._...k,(.Uj....>
FF C5 B9 C4 0C 34 C4 E8 59 7E 19 3A BC B1 3B 57  .....4..Y~.:..;W
ED 4F 99 DF 5E 6D 3D 68 5C 61 EE 8D E9 C2 89 E6  .O..^m=h\a......
E7 59 16 16 FF 6D 93 B0 A8 CE A6 9F 19 52 3A 59  .Y...m.......R:Y
AD 58 63 FE 04 24 77 34 6D BD 75 EC FB EA 23 57  .Xc..$w4m.u...#W
CE DF ED 96 33 6D 64 6A 52 59 0D 5E F2 CB 3B 4B  ....3mdjRY.^..;K
53 59 C5 15 D7 13 81 92 E1 04 A3 4A 4F DA DD 85  SY.........JO...
AA EB 01 5E 8F 5F 2F F6 2B 20 EB 15 5E 9D BB F0  ...^._/.+ ..^...
C3 FF FC 59 23 48 9D 80 C3 EF 03 A1 3F C8 96 6C  ...Y#H......?..l
6F 69 E7 D1 AD 91 EF B0 F7 BE B5 8E 04 40 2F 64  oi..........@/d
F9 34 17 F0 CB AA 91 CA 79 8D 5B F7 00 09 26 C2  .4......y.[...&.
B6 9B 2C B7 2E 6B 68 FA 41 34 2E 8F 15 F8 71 72  ..,..kh.A4....qr
```

```
16 A5 F1 EA ED 71 8D 09 43 03 AF 23 16 03 03 01  .....q..C..#....
2C 0C 00 01 28 03 00 1D 20 F6 35 63 41 20 7B DD  ,...(... .5cA {.
26 BE 86 BC 58 F7 3E 1F D2 43 C1 62 E7 63 1D 8E  &...X.>..C.b.c..
97 81 AB DF 14 33 89 7B 66 06 01 01 00 09 BA 43  .....3.{f......C
80 C1 71 79 83 2D E9 A9 14 1F CE 81 84 D3 BA 0A  ..qy.-..........
04 04 80 DE EF B8 40 D7 8F B2 78 86 56 83 CB 80  ......@...x.V...
4E A0 9D 99 02 58 4F 09 EF EA 7F D0 AD DF 75 93  N....XO.......u.
A4 95 AD 72 15 2A 91 AE 17 1A 17 BE DD F0 AC 89  ...r.*..........
96 61 C7 A9 1D 21 E6 DD 44 03 B9 42 99 BC A5 F4  .a...!..D..B....
41 2E 72 78 ED C7 79 6C A0 65 94 AE 07 68 2F 26  A.rx..yl.e...h/&
C9 55 9C 53 3D 65 72 16 77 96 F6 D2 5A 2E 97 CE  .U.S=er.w...Z...
E0 F2 CA 3A A0 AC 2C 7C 33 D4 E5 22 93 6A 83 58  ...:..,|3..".j.X
76 14 4A B4 5F 28 99 BF 8B E4 29 6F 08 9E 49 79  v.J._(....)o..Iy
AD 75 64 D6 F6 10 58 D1 D9 A2 AD A4 44 B0 CB A7  .ud...X.....D...
C5 7C 8C 48 2C 84 47 5E 0E 87 E2 3C 02 6A B3 A1  .|.H,.G^...<.j..
89 5E 21 49 73 54 E8 15 94 ED 6A 19 EE B7 A6 17  .^!IsT....j.....
B5 DC 18 AE 99 94 4B 1B 21 33 CF B1 DF 5F 08 07  ......K.!3..._..
AE CA 57 80 F2 25 D0 D4 8D 9F ED F3 BE F6 BB 26  ..W..%.........&
23 3C F9 8C 1C 17 DE F9 DD FF 7E D2 D7 C8 51 91  #<........~...Q.
A1 27 85 D1 58 6D 69 C2 8A D5 4B 85 E9 16 03 03  .'..Xmi...K.....
00 04 0E 00 00 00                                ......
```

IDS Rules Detection mechanism:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)"; flow:established,from_server; content:"|16|"; content:"|0b|"; within:8; content:"|09 00|"; within:30; content:"|55 04 0a|"; distance:0; content:"|0f|Global Security"; distance:1; within:16; fast_pattern; content:"|55 04 0b|"; distance:0; content:"|0d|IT Department"; distance:1; within:14; content:"|55 04 03|"; distance:0; content:"|0b|example."; distance:1; within:9; metadata: former_category MALWARE; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2021013; rev:6; metadata:attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2015_04_27, updated_at 2018_05_17;)
```

Win.Trojan.Emotet variant

Infected Payload with signature marked:

```
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A  GET / HTTP/1.1..
43 6F 6F 6B 69 65 3A 20 31 35 36 38 30 3D 57 47  Cookie: 15680=WG
61 32 37 76 61 76 32 7A 51 2B 71 4A 4B 2F 6B 6F  a27vav2zQ+qJK/ko
61 76 76 6E 62 42 69 6E 57 42 6E 77 48 30 30 64  avvnbBinWBnwH00d
6F 61 6B 62 49 75 43 4B 6B 73 7A 76 49 4C 30 66  oakbIuCKkszvIL0f
62 47 39 7A 38 46 6E 66 53 42 43 2F 6C 54 36 71  bG9z8FnfSBC/lT6q
61 6F 79 69 72 43 4F 79 4C 47 74 52 67 30 50 5A  aoyirCOyLGtRg0PZ
64 72 35 34 49 61 4E 33 4A 71 4E 33 2B 57 39 42  dr54IaN3JqN3+W9B
75 48 79 44 51 35 32 59 37 39 57 50 69 30 76 6F  uHyDQ52Y79WPi0vo
54 54 4A 33 72 57 47 46 4C 5A 30 4E 43 32 2F 53  TTJ3rWGFLZ0NC2/S
72 6D 52 62 2F 6D 4A 34 7A 43 39 43 45 42 4A 4E  rmRb/mJ4zC9CEBJN
50 59 49 33 35 63 4A 55 31 38 75 53 64 55 69 63  PYI35cJU18uSdUic
70 75 2F 50 37 74 32 62 7A 4C 2B 32 4A 30 4E 52  pu/P7t2bzL+2J0NR
48 61 46 64 59 66 73 33 30 2F 30 6F 75 69 56 4E  HaFdYfs30/0ouiVN
75 2B 2B 63 33 57 71 31 64 6E 34 70 6A 55 72 72  u++c3Wq1dn4pjUrr
42 6E 38 4D 54 4B 75 52 61 6C 62 47 43 64 54 2F  Bn8MTKuRalbGCdT/
44 2B 5A 7A 2B 5A 48 65 77 79 68 37 2F 74 4D 2F  D+Zz+ZHewyh7/tM/
67 4E 6A 34 44 6A 74 7A 6B 74 75 4E 53 43 4A 51  gNj4DjtzktuNSCJQ
37 4C 63 47 6D 52 56 36 2F 68 72 74 79 44 76 58  7LcGmRV6/hrtyDvX
67 4E 46 63 34 6E 73 4A 73 6B 47 67 4D 6A 48 33  gNFc4nsJskGgMjH3
48 66 4F 4D 78 53 68 6A 59 59 5A 36 67 59 62 69  HfOMxShjYYZ6gYbi
46 33 54 6A 48 37 7A 6B 31 6F 4A 34 73 57 62 73  F3TjH7zk1oJ4sWbs
44 38 4B 4A 6B 74 69 57 6E 61 42 47 4D 51 37 75  D8KJktiWnaBGMQ7u
79 76 6D 76 51 43 4E 43 45 77 59 58 7A 69 73 58  yvmvQCNCEwYXzisX
37 34 7A 4A 57 2B 32 70 47 67 4E 62 45 58 57 65  74zJW+2pGgNbEXWe
52 76 48 61 30 63 75 57 36 30 76 66 42 6C 49 46  RvHa0cuW60vfBlIF
4C 4E 48 34 59 32 45 56 4C 57 4A 56 36 71 33 2F  LNH4Y2EVLWJV6q3/
4B 51 2F 45 79 72 36 4D 79 39 61 38 59 49 4F 4C  KQ/Eyr6My9a8YIOL
45 73 42 67 69 37 73 78 4D 52 72 55 48 4B 0D 0A  EsBgi7sxMRrUHK..
55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69  User-Agent: Mozi
6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 69  lla/4.0 (compati
62 6C 65 3B 20 4D 53 49 45 20 37 2E 30 3B 20 57  ble; MSIE 7.0; W
69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57  indows NT 6.1; W
4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E  OW64; Trident/7.
30 3B 20 53 4C 43 43 32 3B 20 2E 4E 45 54 20 43  0; SLCC2; .NET C
4C 52 20 32 2E 30 2E 35 30 37 32 37 3B 20 2E 4E  LR 2.0.50727; .N
45 54 20 43 4C 52 20 33 2E 35 2E 33 30 37 32 39  ET CLR 3.5.30729
3B 20 2E 4E 45 54 20 43 4C 52 20 33 2E 30 2E 33  ; .NET CLR 3.0.3
30 37 32 39 3B 20 4D 65 64 69 61 20 43 65 6E 74  0729; Media Cent
65 72 20 50 43 20 36 2E 30 3B 20 2E 4E 45 54 34  er PC 6.0; .NET4
2E 30 43 3B 20 2E 4E 45 54 34 2E 30 45 29 0D 0A  .0C; .NET4.0E)..
48 6F 73 74 3A 20 38 37 2E 36 36 2E 31 33 2E 38  Host: 87.66.13.8
30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B  0..Connection: K
65 65 70 2D 41 6C 69 76 65 0D 0A 43 61 63 68 65  eep-Alive..Cache
2D 43 6F 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63  -Control: no-cac
68 65 0D 0A 0D 0A                                he....
```

Snort Detection mechanism:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"MALWARE-CNC
Win.Trojan.Emotet variant outbound connection attempt"; flow:to_server,established;
content:"GET / HTTP/1.1|0D 0A|Cookie: "; depth:24; content:"="; within:6; pcre:"/Cookie:
\d{1,5}=[a-zA-Z0-9\x2b\x2f]+=*\r\nUser-Agent:/"; metadata:impact_flag red, policy
balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service http;
reference:url,attack.mitre.org/techniques/T1041/;
reference:url,www.virustotal.com/en/file/f78b1778da8108d3a9d3ca5d8194fb607d9fe84d
a4aabbfec0c27f5d261cd646/analysis/; classtype:trojan-activity; sid:48402; rev:1;)
```

Trojan.Trickbot self-signed certificate exchange

Infected Payload with signature marked:

```
16 03 01 00 59 02 00 00 55 03 01 36 CC C2 26 A8  ....Y...U..6..&.
F5 F9 52 4B 61 5A FB 0E B2 DF 82 A0 96 26 D9 49  ..RKaZ.......&.I
5D BE E0 9B B0 E1 E2 33 F5 76 22 20 16 8A BE EF  ]......3.v" ....
```

```
3C 24 D7 20 A0 A9 E1 ED FE AE C9 EC C1 D6 11 38  <$. ...........8
0D 76 FB 8A 64 C3 F5 AE 34 47 C2 88 C0 14 00 00  .v..d...4G......
0D FF 01 00 01 00 00 0B 00 04 03 00 01 02 16 03  ................
01 03 6E 0B 00 03 6A 00 03 67 00 03 64 30 82 03  ..n...j..g..d0..
60 30 82 02 48 A0 03 02 01 02 02 09 00 F7 F3 C8  `0..H...........
AE E0 B8 CD 22 30 0D 06 09 2A 86 48 86 F7 0D 01  ...."0...*.H....
01 0B 05 00 30 45 31 0B 30 09 06 03 55 04 06 13  ....0E1.0...U...
02 41 55 31 13 30 11 06 03 55 04 08 0C 0A 53 6F  .AU1.0...U....So
6D 65 2D 53 74 61 74 65 31 21 30 1F 06 03 55 04  me-State1!0...U.
0A 0C 18 49 6E 74 65 72 6E 65 74 20 57 69 64 67  ...Internet Widg
69 74 73 20 50 74 79 20 4C 74 64 30 1E 17 0D 31  its Pty Ltd0...1
38 30 39 32 34 31 35 32 34 35 33 5A 17 0D 31 39  80924152453Z..19
30 39 32 34 31 35 32 34 35 33 5A 30 45 31 0B 30  0924152453Z0E1.0
09 06 03 55 04 06 13 02 41 55 31 13 30 11 06 03  ...U....AU1.0...
55 04 08 0C 0A 53 6F 6D 65 2D 53 74 61 74 65 31  U....Some-State1
21 30 1F 06 03 55 04 0A 0C 18 49 6E 74 65 72 6E  !0...U....Intern
65 74 20 57 69 64 67 69 74 73 20 50 74 79 20 4C  et Widgits Pty L
74 64 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D  td0.."0...*.H...
01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82  ..........0.....
01 01 00 D9 5D D0 D6 D3 2A 15 F2 16 08 58 1A 63  ....]...*....X.c
C6 8D 3D B8 FC 65 5B 69 DF 22 9A 3D E4 E9 A1 B8  ..=..e[i.".=....
0C AE B1 EC 10 76 55 F2 41 F3 0C 18 8C 57 FB AB  .....vU.A....W..
2C 69 5C 78 5C 37 65 0A 47 13 08 B9 86 3C 8C 7D  ,i\x\7e.G....<.}
22 D8 BE 5A E6 02 65 65 7B 79 3F F6 7B 86 D8 C9  "..Z..ee{y?.{...
4F F7 70 5C 68 A2 10 7E E7 A5 21 F5 9A FD E6 F9  O.p\h..~..!.....
73 75 3D 89 35 EA 60 64 01 14 10 53 7A BF E4 72  su=.5.`d...Sz..r
7D 08 C8 FE A2 8C F2 DA FE 72 AA 18 A3 97 C5 86  }.........r......
FD 46 49 CE D4 48 B6 A7 44 BF 68 87 FC E0 FB 2B  .FI..H..D.h....+
9A 62 DE 68 FB 8B 7A C5 3E 37 5C D7 68 D6 E0 BD  .b.h..z.>7\.h...
8E EA 99 8A A4 19 E8 A6 28 5A 94 42 94 19 19 02  ........(Z.B....
6F AC 09 88 E1 02 E7 5C 33 FD C4 87 A6 E5 07 60  o......\3......`
AE 36 36 84 33 46 AF A0 D8 CE AA 0D 28 9F D4 34  .66.3F......(..4
E9 AA 22 FF 17 19 AC 6F AA E9 1F 6D D6 B1 DE CC  .."....o...m....
64 F5 71 81 91 F5 EB 7C C1 8B C3 6E B5 AD 43 F9  d.q....|...n..C.
37 A6 33 80 D3 C7 79 BD BA 3B 08 86 D4 B9 37 AC  7.3...y..;....7.
```

```
C3 E6 A9 02 03 01 00 01 A3 53 30 51 30 1D 06 03  .........S0Q0...
55 1D 0E 04 16 04 14 17 1A A3 FF B4 45 28 C2 FC  U..........E(..
7A 52 FB B3 04 3D 04 D7 E4 CF F4 30 1F 06 03 55  zR...=.....0...U
1D 23 04 18 30 16 80 14 17 1A A3 FF B4 45 28 C2  .#..0........E(.
FC 7A 52 FB B3 04 3D 04 D7 E4 CF F4 30 0F 06 03  .zR...=.....0...
55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0D 06  U.......0....0..
09 2A 86 48 86 F7 0D 01 01 0B 05 00 03 82 01 01  .*.H...........
00 72 68 B3 60 B3 8E F2 D1 A5 53 73 A3 D7 5D 56  .rh.`.....Ss..]V
C4 4E EB 5A A2 46 1E E2 1F DA 3C 9A 47 DD 98 5B  .N.Z.F....<.G..[
B1 7E BD 9F 88 33 51 90 8C 31 DF 31 A2 D5 48 92  .~...3Q..1.1..H.
EE 46 35 78 C0 87 AC DE EF 1E CA 6E E4 3A 31 1A  .F5x.......n.:1.
01 FA DF 8B 08 03 DE 6A 1D FF C9 9C E9 B3 65 D9  .......j......e.
50 BC 84 9D BC 3D E2 B2 77 DB 42 78 2E 15 56 38  P....=..w.Bx..V8
3F BF DC 90 A1 87 00 3D 83 41 4D AA D0 BF 8C 04  ?......=.AM.....
52 4E 4F 67 C7 15 9A 2E 4F 0A FD 77 31 6F BC 79  RNOg....O..w1o.y
C8 D9 96 48 67 C9 B2 BE 88 0E E6 DF C4 E4 61 61  ...Hg.........aa
C4 61 F4 36 B6 5A 25 87 EC 50 3F B7 1D 2C 49 54  .a.6.Z%..P?..,IT
9B 78 EE B3 EB C8 71 C0 35 70 19 CA A4 C2 EC E1  .x....q.5p......
22 FF 9D 89 B7 15 B7 B0 DD 78 E0 46 5A 99 A0 10  "........x.FZ...
1F D1 46 04 40 28 3E 95 74 D1 B4 29 2F 86 AF 8C  ..F.@(>.t..)/...
8E 41 1C D4 44 8B 19 B6 F4 A7 F9 4C FE 65 27 7B  .A..D......L.e'{
5F 69 24 82 F1 C9 9F 3C 31 AC B4 29 75 7B F7 3D  _i$....<1..)u{.=
E6 98 88 B8 79 A5 B6 3F 51 58 72 32 13 98 23 85  ....y..?QXr2..#.
89 16 03 01 01 4B 0C 00 01 47 03 00 17 41 04 A5  .....K...G...A..
1A 8E 05 9E 03 EE EF 8B D6 DA 10 50 1F C4 37 C0  ..........P..7.
3A D8 24 AB 65 48 EA C1 26 EB 38 B8 50 30 54 07  :.$.eH..&.8.P0T.
16 B6 11 ED 95 18 1E 94 DC 00 53 90 C1 CB A1 5B  ..........S....[
38 19 7D BA A3 79 06 3D EE 7C AD 89 38 46 72 01  8.}..y.=.|..8Fr.
00 27 22 4B AD 7A 9A 81 F0 4E 74 F9 E0 C7 2A 18  .'"K.z...Nt...*.
97 D0 5E BB 5D EC 08 C8 6F 64 13 37 EA 78 31 EE  ..^.]...od.7.x1.
E8 42 81 0A A6 D4 A1 59 C9 54 03 C4 69 E6 1C 66  .B.....Y.T..i..f
49 F6 C5 51 E3 8D E5 B5 49 04 3E 4F 49 B5 BB A4  I..Q....I.>OI...
5A 5B 51 20 FF 14 0E 39 C5 AE 60 A0 C6 C5 EA FA  Z[Q ...9..`.....
9B 40 8B 5E A6 64 19 5F 08 38 14 CD D4 D5 A6 17  .@.^.d._.8......
21 D5 EC BE FD 6B 1D 0B 52 2E 51 43 A0 B5 8E 69  !....k..R.QC...i
```

```
86 10 60 5E 3E B2 DC BA CF 93 AB 08 5F 7A 97 AC  ..`^>......._z..
51 09 85 D0 D4 DE 69 2C AF B7 01 F4 E5 32 00 21  Q.....i,.....2.!
71 68 1D 5F DE EF 04 2F C2 15 BD D4 27 D3 2F C7  qh._.../....'./.
2D 01 BF 2F BC 48 71 E3 8C 03 0E A7 60 58 F8 ED  -../.Hq.....`X..
95 F3 BF C3 85 F4 7E D5 D7 08 39 25 EB FA 61 B3  ......~...9%..a.
8C 0E AB 15 09 F1 84 15 7D 1A 48 19 9B F8 25 96  ........}.H...%.
7A 59 43 61 E6 0D F4 4D 16 44 20 C2 AE 7B 27 95  zYCa...M.D ..{'.
B4 F2 0C 57 20 7E 1E 00 83 78 5C 11 F1 23 6B 44  ...W ~...x\..#kD
4E 0D B7 12 83 C4 53 2B C9 B8 3C 2E C3 98 8A C8  N.....S+..<.....
59 16 03 01 00 04 0E 00 00 00                    Y.........
```

Snort detection mechanism:

```
alert tcp $EXTERNAL_NET [443,447,449] -> $HOME_NET any (msg:"MALWARE-OTHER
Win.Trojan.Trickbot self-signed certificate exchange attempt"; flow:to_client,established;
content:"|F7 F3 C8 AE E0 B8 CD 22|"; fast_pattern:only; content:"Internet Widgits Pty Ltd";
metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips drop, policy
security-ips drop, service ssl;
reference:url,virustotal.com/#/file/3a1692a6d0f6881b45792dfc4649b166965744b3d3877
84494d67874cd5d379b; classtype:trojan-activity; sid:50714; rev:1;)
```

References

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

https://blog.talosintelligence.com/2020/03/trickbot-primer.html#more

https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

https://spanning.com/blog/ryuk-ransomware-malware-of-the-month/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response

https://dsimg.ubm-us.net/envelope/401393/577263/emotet-survival-handbook%20.pdf

ōrdr

info@ordr.net

www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054