Cert Safari: Leveraging TLS Certificates to Hunt Evil

prevailion.com/cert-safari-leveraging-tls-certificates-to-hunt-evil/

July 27, 2021

27 July 2021

Proactively hunting for malicious infrastructure is a persistent puzzle for threat researchers to work and solve. It is a complex and evolving problem, made more complex (though not unmanageable) by Domain Privacy and GDPR, which obscure WHOIS information that

Analysts and Researchers would otherwise use to identify trends and corroborate other observations to increase confidence in attribution of infrastructure clustering. This has forced researchers to identify other methods to proactively hunt for malicious infrastructure.

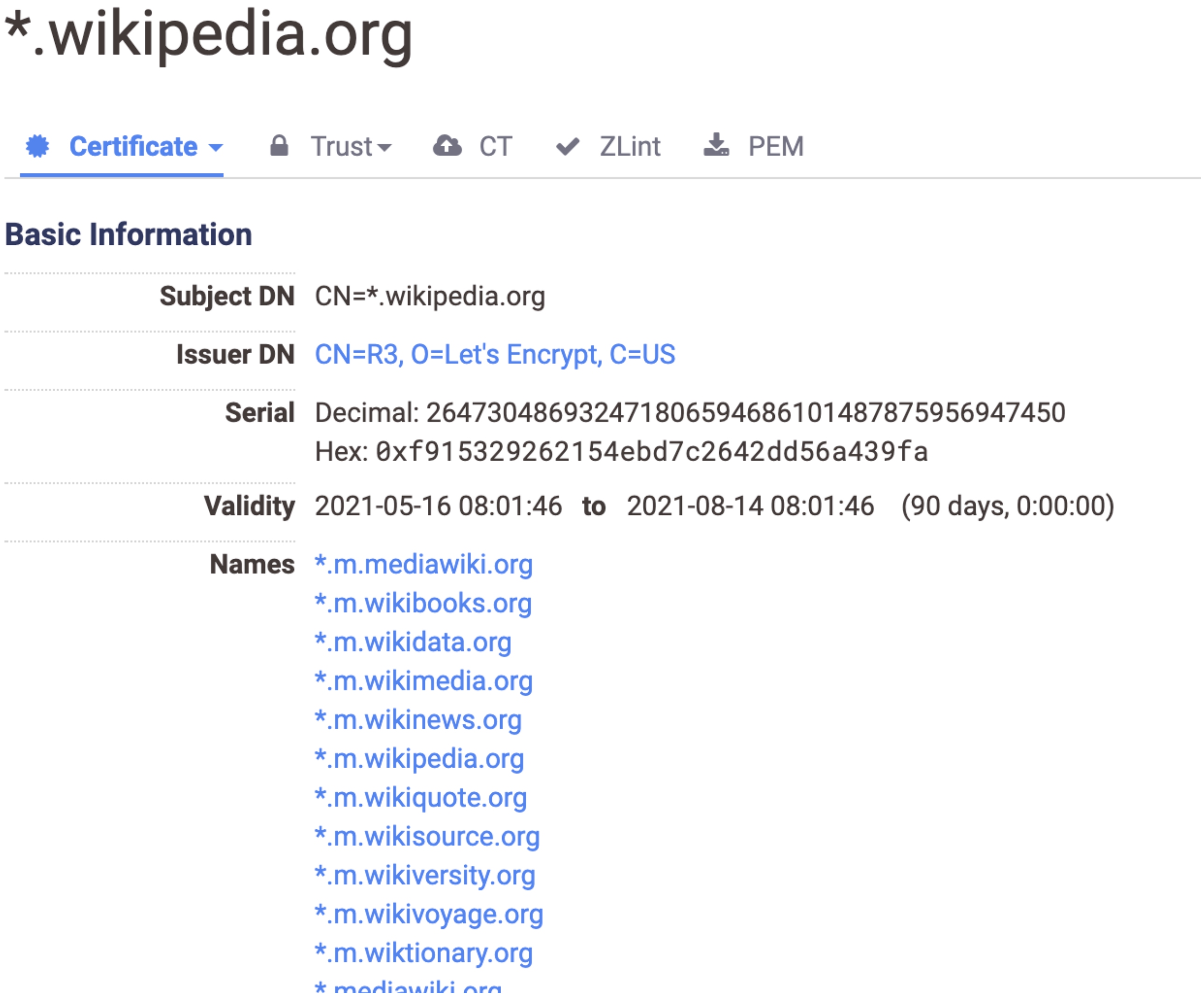
How to Leverage TLS Certificates

Assisted by an increasing body of knowledge generated by thoughtful, forward-leaning analysts working on this very problem {1-9}, the Prevailion Adversarial Counterintelligence Team (PACT) leverages TLS certificates to compensate for the investigatory vacuum left by WHOIS redactions. But, before we dive into an analytical methodology along with an example that leverages this source of information, a quick primer on how the internet works:

- Domain names, like "Wikipedia.org," are not required for network communications, but an IP address is (the internet runs on TCP/IP, after all).
- Domain names provide a sense of brand, recognition, and utility that IP addresses cannot (IP addresses are for machines, domain names are for people).
- Most legitimate sites will have a domain name that is mapped to (one or more) IP addresses.

The push for encrypted communications over the internet, mainly due to the influence of ecommerce, made much of the day-to-day communications between a user's computer and a website (on a domain) encrypted using the TLS (Transport Layer Security) protocol. To implement and use TLS, a website must first prove its identity by presenting a TLS certificate. The TLS certificate contains information about the website (domain) and the organization that runs and owns that domain. It is further countersigned by a trusted party (the Certificate Authority, or CA), whose sole job is to verify that the site is truly owned and operated by the entity claiming ownership.

TLS certs are intended to bind together a domain name with an organizational identity {10}. For example, the TLS cert for Wikipedia {Figure 1, below} displays the Subject Common Name (CN=*.wikipedia.org), effectively proving the web server's legitimate right to serve any webpage from the domain (or any subdomain) ending in "wikipedia.org". Additionally, it can serve web pages from the other domains on the cert, as agreed upon by the entity (Wikipedia) and the CA (Let's Encrypt).



*.wikipedia.org

Basic Information

Subject DN CN=*.wikipedia.org

Issuer DN CN=R3, O=Let's Encrypt, C=US

Serial Decimal: 264730486932471806594686101487875956947450
Hex: 0xf915329262154ebd7c2642dd56a439fa

Validity 2021-05-16 08:01:46 **to** 2021-08-14 08:01:46 (90 days, 0:00:00)

Names *.m.mediawiki.org
*.m.wikibooks.org
*.m.wikidata.org
*.m.wikimedia.org
*.m.wikinews.org
*.m.wikipedia.org
*.m.wikiquote.org
*.m.wikisource.org
*.m.wikiversity.org
*.m.wikivoyage.org
*.m.wiktionary.org
*.mediawiki.org

Figure 1 – Wikpedia's TLS certificate

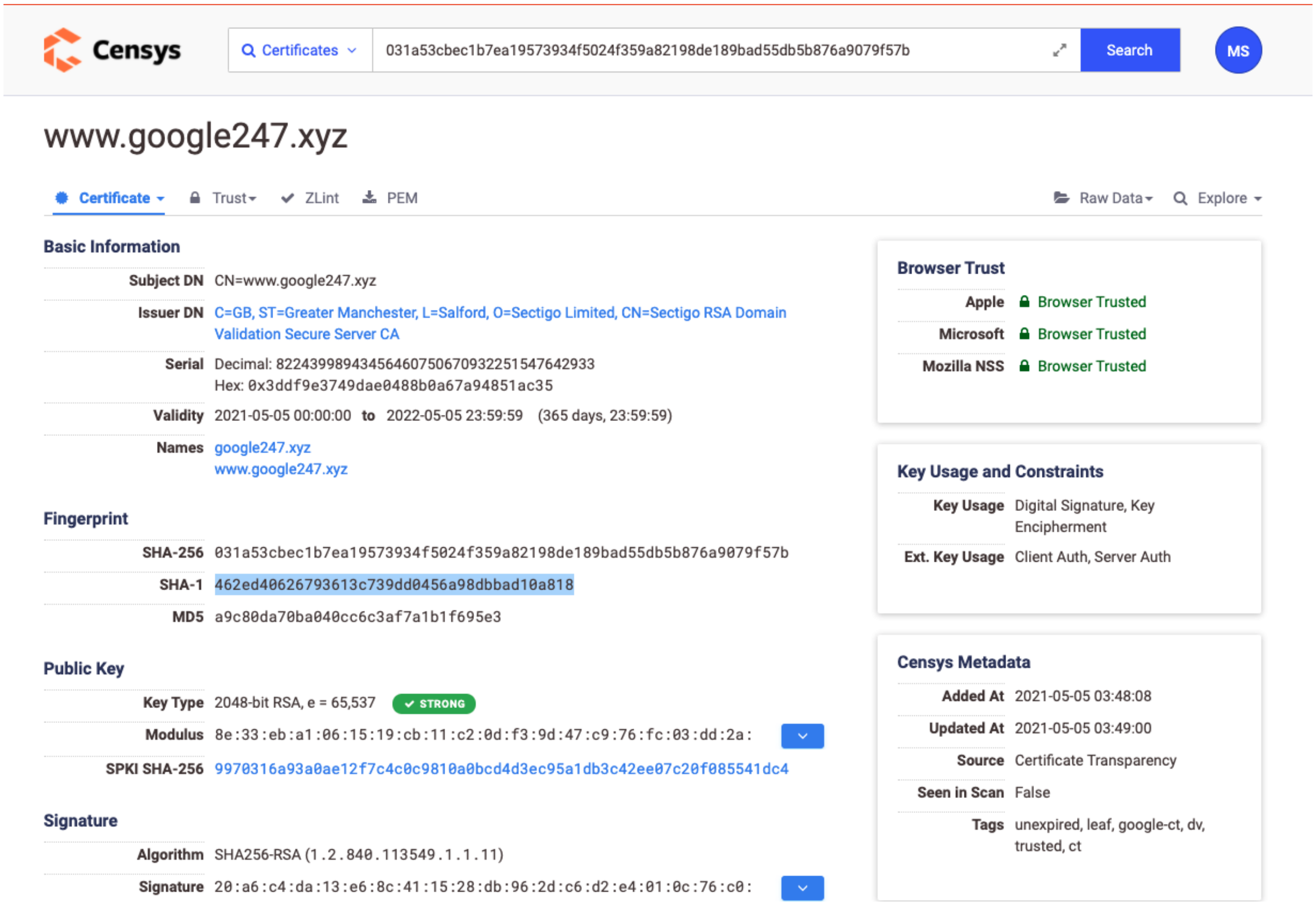
Armed with the understanding that TLS certificates are required for encrypted communications between a computer and a website (domain), and that IP addresses are required for network communications (but domain names are not), it stands to reason that TLS certificates must be associated with the IP addresses hosting a given domain.

Malicious actors must execute most, if not all, of the following steps to create supporting infrastructure for their operations {7}:

1. Create a registration persona
2. Buy a domain name from a registrar/reseller
3. Set up hosting at an IP address
4. Set up target or operation-specific subdomain infrastructure
5. Create an SSL certificate if requiring HTTPS communication
6. Enable services at a hosting IP address or the domain
7. Set up domain with a website or redirect

Each of these steps provides an opportunity for the researcher to identify tactics or artifacts that can be used to cluster adversary activity or infrastructure. This methodology was recently used by the PACT to uncover what appears to be a cluster of unattributed activity that has yet to be reported on, hosted mainly on Vietnamese infrastructure and using domain names with a technology and cryptocurrency theme.

The PACT initially identified a blacklisted certificate, listed as a generic "Malware C&C," on the SSL certificate blacklist (SSLBL) provided by the amazing folks at ABUSE.ch {11}. Analysts identified the cert on Censys.io by its SHA1 fingerprint, where it was associated with "google247[.]xyz" {Figure 2 below}



031a53cbec1b7ea19573934f5024f359a82198de189bad55db5b876a9079f57b

www.google247.xyz

Basic Information

Subject DN	CN=www.google247.xyz
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	Decimal: 82243998943456460750670932251547642933 Hex: 0x3ddf9e3749dae0488b0a67a94851ac35
Validity	2021-05-05 00:00:00 **to** 2022-05-05 23:59:59 (365 days, 23:59:59)
Names	google247.xyz www.google247.xyz

Fingerprint

SHA-256	031a53cbec1b7ea19573934f5024f359a82198de189bad55db5b876a9079f57b
SHA-1	462ed40626793613c739dd0456a98dbbad10a818
MD5	a9c80da70ba040cc6c3af7a1b1f695e3

Public Key

Key Type	2048-bit RSA, e = 65,537 ✓ STRONG
Modulus	8e:33:eb:a1:06:15:19:cb:11:c2:0d:f3:9d:47:c9:76:fc:03:dd:2a:
SPKI SHA-256	9970316a93a0ae12f7c4c0c9810a0bcd4d3ec95a1db3c42ee07c20f085541dc4

Signature

Algorithm	SHA256-RSA (1.2.840.113549.1.1.11)
Signature	20:a6:c4:da:13:e6:8c:41:15:28:db:96:2d:c6:d2:e4:01:0c:76:c0:

Browser Trust

Apple	Browser Trusted
Microsoft	Browser Trusted
Mozilla NSS	Browser Trusted

Key Usage and Constraints

Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Client Auth, Server Auth

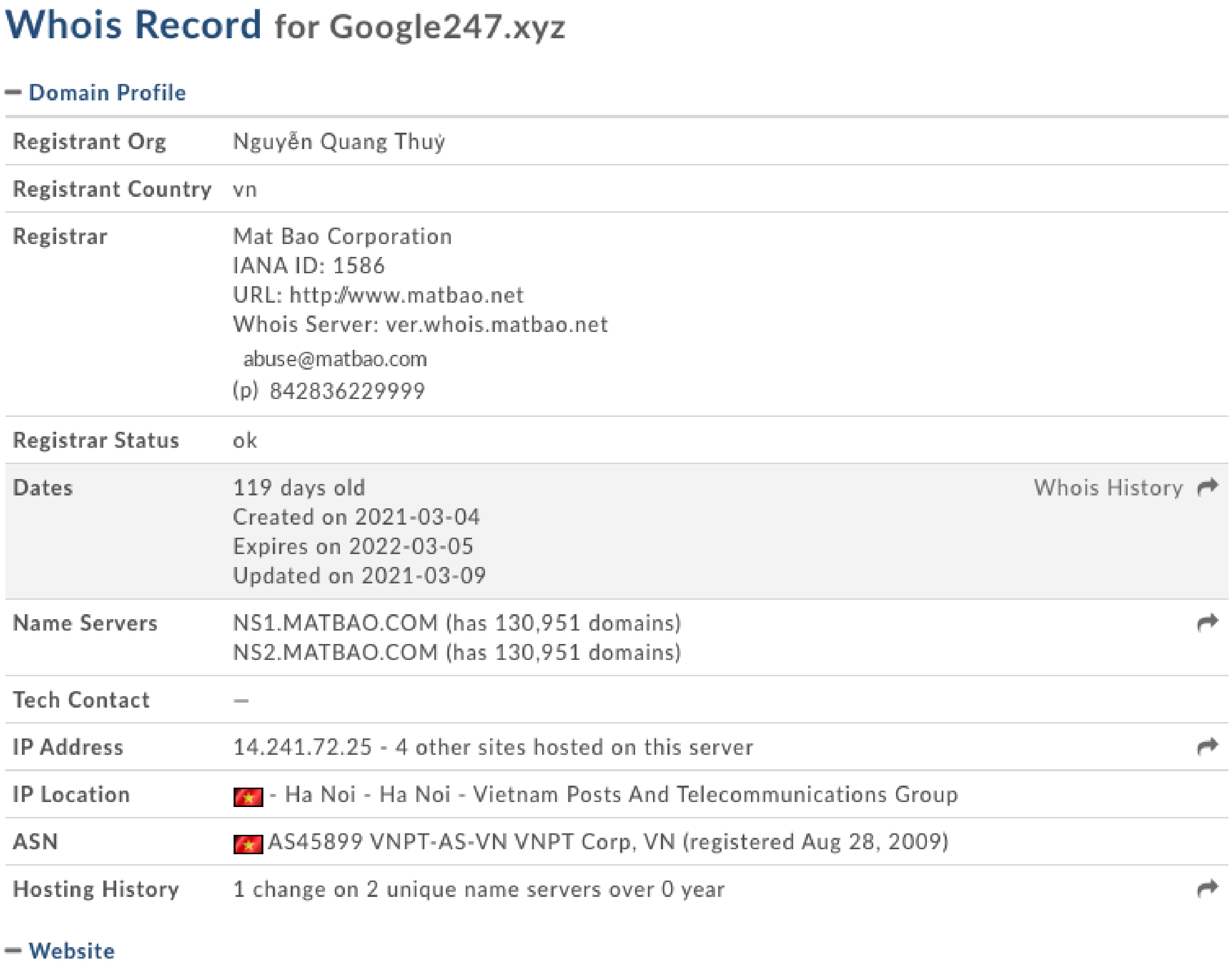
Censys Metadata

Added At	2021-05-05 03:48:08
Updated At	2021-05-05 03:49:00
Source	Certificate Transparency
Seen in Scan	False
Tags	unexpired, leaf, google-ct, dv, trusted, ct

Figure 2 – the blacklisted certificate from SSLBL

To identify the hosting infrastructure, analysts used DomainTools' WHOIS tool to query the domain associated with the certificate. Two notable facts were identified:

1. The domain is hosted on 14.241.72[.]25
2. Four other domains are hosted on the same IP {Figure 3, below}.



Whois Record for Google247.xyz

— Domain Profile

Registrant Org	Nguyễn Quang Thuỳ
Registrant Country	vn
Registrar	Mat Bao Corporation IANA ID: 1586 URL: http://www.matbao.net Whois Server: ver.whois.matbao.net abuse@matbao.com (p) 842836229999
Registrar Status	ok
Dates	119 days old Created on 2021-03-04 Expires on 2022-03-05 Updated on 2021-03-09 Whois History
Name Servers	NS1.MATBAO.COM (has 130,951 domains) NS2.MATBAO.COM (has 130,951 domains)
Tech Contact	–
IP Address	14.241.72.25 - 4 other sites hosted on this server
IP Location	- Ha Noi - Ha Noi - Vietnam Posts And Telecommunications Group
ASN	AS45899 VNPT-AS-VN VNPT Corp, VN (registered Aug 28, 2009)
Hosting History	1 change on 2 unique name servers over 0 year

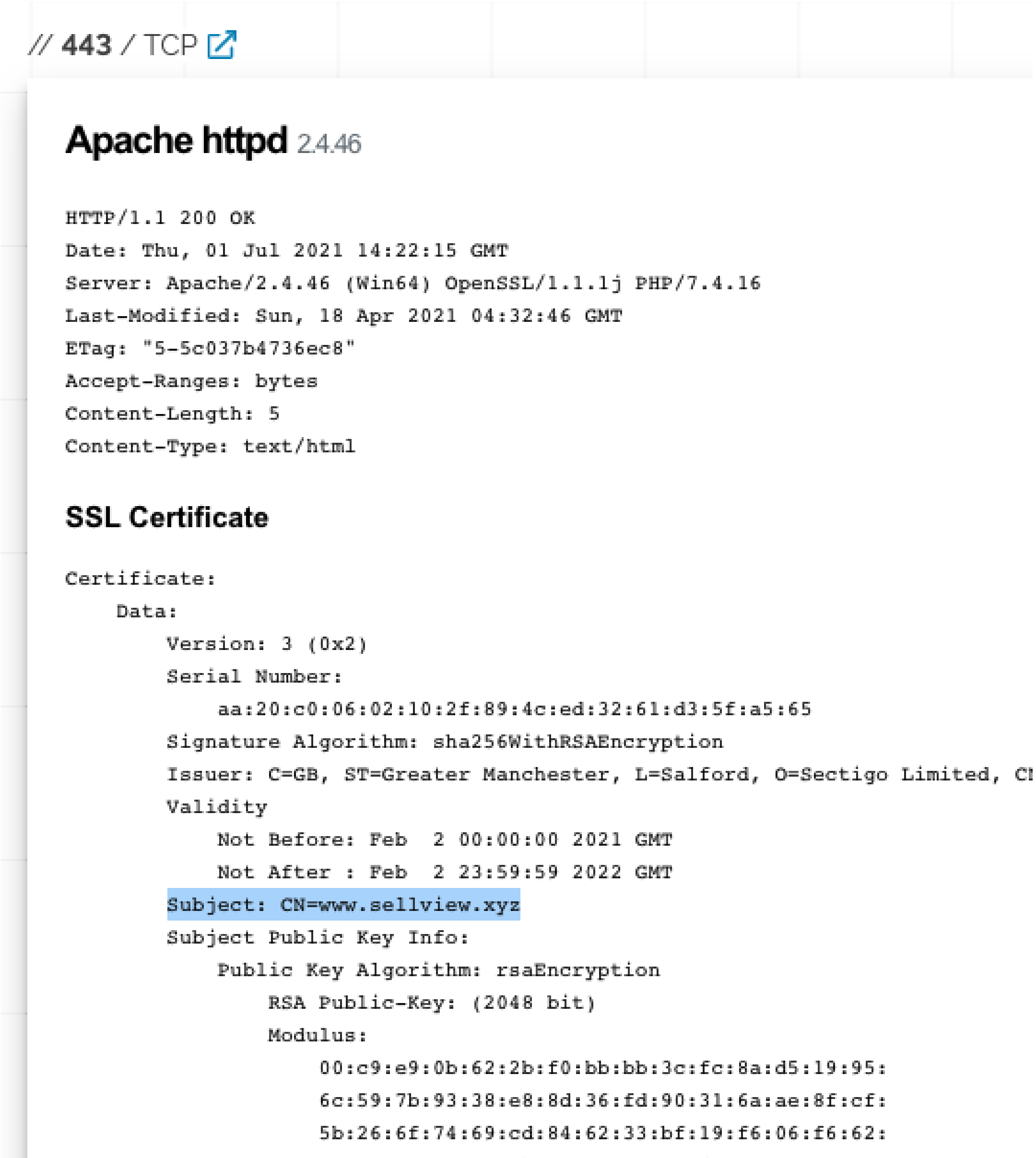
— Website

Figure 3 – WHOIS info for the domain associated with the blacklisted certificate

Analysts also noted the following additional facts for future pivots:

1. Registrant Organization: Nguyễn Quang Thuỷ
2. Registrar: Mat Bao Corporation
3. Name Servers: NS1.MATBAO.COM & NS2.MATBAO.COM

Identifying the hosting address of the domain enabled a pivot to Shodan {Figures 4,5, below}, which identified an additional domain associated with that IP: sellview[.]xyz.



Apache httpd 2.4.46

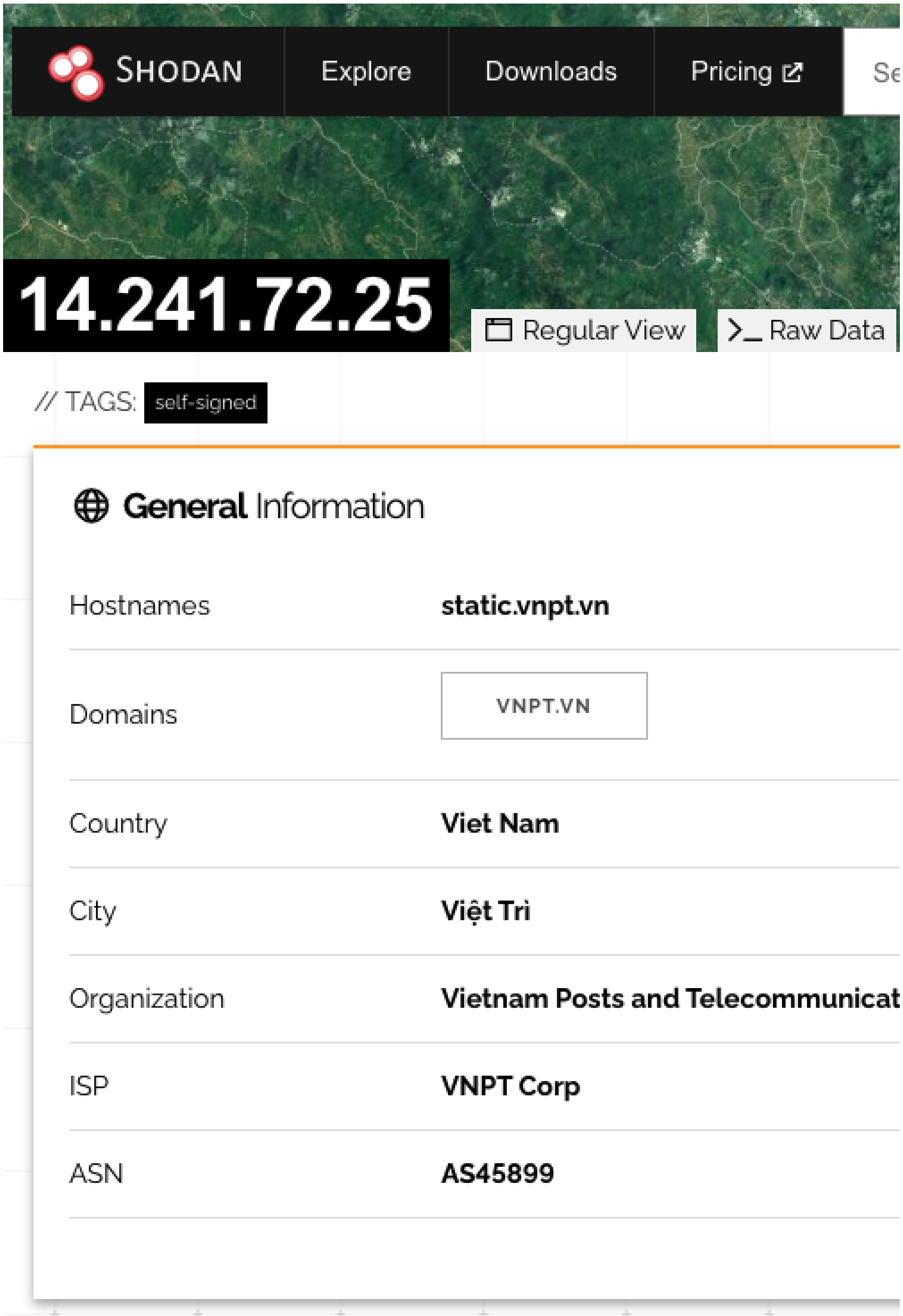
```
HTTP/1.1 200 OK
Date: Thu, 01 Jul 2021 14:22:15 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.4.16
Last-Modified: Sun, 18 Apr 2021 04:32:46 GMT
ETag: "5-5c037b4736ec8"
Accept-Ranges: bytes
Content-Length: 5
Content-Type: text/html
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            aa:20:c0:06:02:10:2f:89:4c:ed:32:61:d3:5f:a5:65
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN
        Validity
            Not Before: Feb  2 00:00:00 2021 GMT
            Not After : Feb  2 23:59:59 2022 GMT
        Subject: CN=www.sellview.xyz
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c9:e9:0b:62:2b:f0:bb:bb:3c:fc:8a:d5:19:95:
                    6c:59:7b:93:38:e8:8d:36:fd:90:31:6a:ae:8f:cf:
                    5b:26:6f:74:69:cd:84:62:33:bf:19:f6:06:f6:62:
```

Figure 4,5 – Results of Shodan query for the host, identifying it by IP and TLS certificate

Censys was used to backstop the findings from Shodan, positively identifying both the IP and the certificate seen on the target IP in Shodan {Figures 6,7, below}:

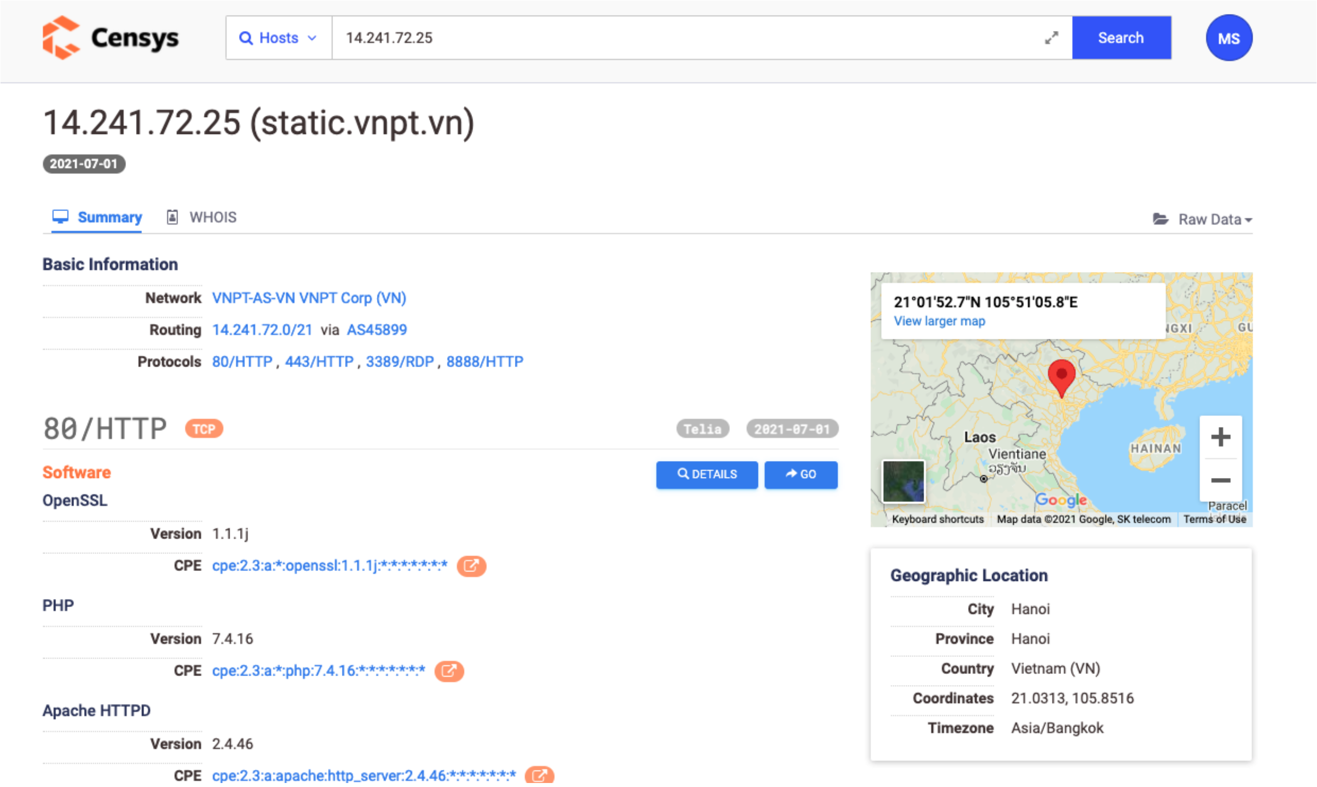


14.241.72.25

// TAGS: self-signed

General Information

Hostnames	**static.vnpt.vn**
Domains	VNPT.VN
Country	**Viet Nam**
City	**Việt Trì**
Organization	**Vietnam Posts and Telecommunicat**
ISP	**VNPT Corp**
ASN	**AS45899**



14.241.72.25 (static.vnpt.vn)

2021-07-01

Basic Information

Network	VNPT-AS-VN VNPT Corp (VN)
Routing	14.241.72.0/21 via AS45899
Protocols	80/HTTP , 443/HTTP , 3389/RDP , 8888/HTTP

80/HTTP TCP Telia 2021-07-01

Software

OpenSSL

Version	1.1.1j
CPE	cpe:2.3:a:*:openssl:1.1.1j:*:*:*:*:*:*:*

PHP

Version	7.4.16
CPE	cpe:2.3:a:*:php:7.4.16:*:*:*:*:*:*:*

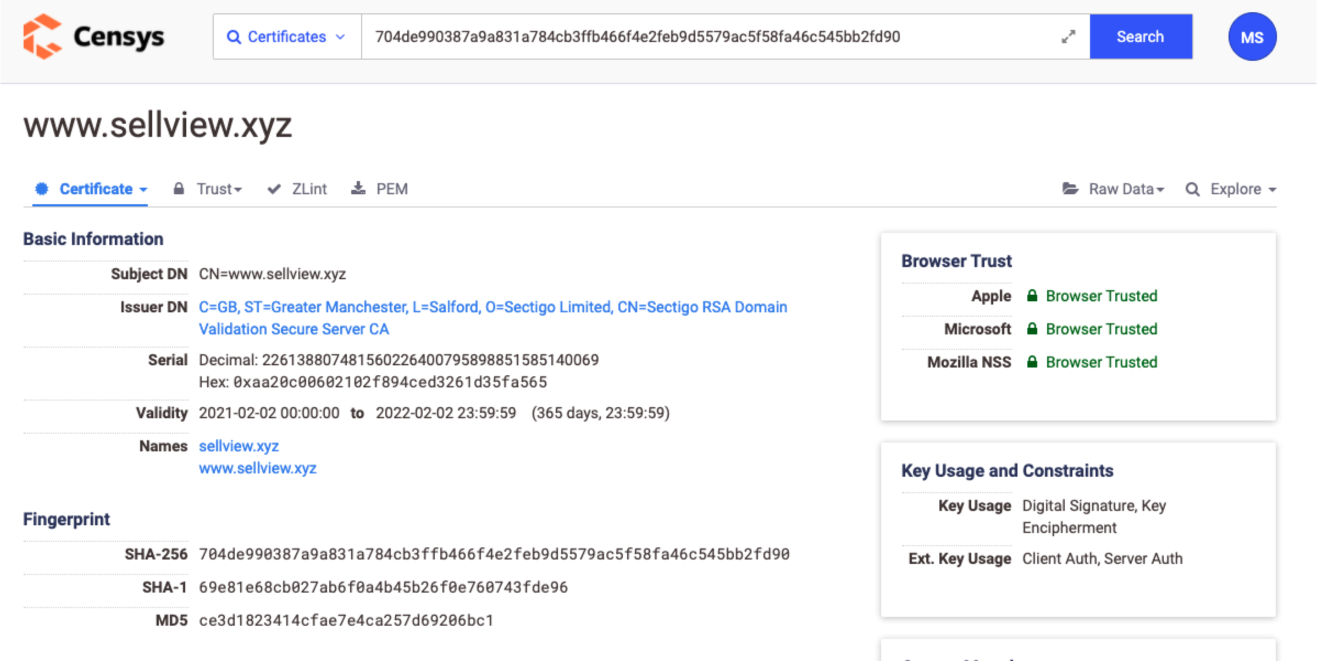
Apache HTTPD

Version	2.4.46
CPE	cpe:2.3:a:apache:http_server:2.4.46:*:*:*:*:*:*:*

Geographic Location

City	Hanoi
Province	Hanoi
Country	Vietnam (VN)
Coordinates	21.0313, 105.8516
Timezone	Asia/Bangkok

Figure 6 – IP corroboration from Censys



www.sellview.xyz

Basic Information

Subject DN	CN=www.sellview.xyz
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	Decimal: 226138807481560226400795898851585140069 Hex: 0xaa20c00602102f894ced3261d35fa565
Validity	2021-02-02 00:00:00 to 2022-02-02 23:59:59 (365 days, 23:59:59)
Names	sellview.xyz www.sellview.xyz

Fingerprint

SHA-256	704de990387a9a831a784cb3ffb466f4e2feb9d5579ac5f58fa46c545bb2fd90
SHA-1	69e81e68cb027ab6f0a4b45b26f0e760743fde96
MD5	ce3d1823414cfae7e4ca257d69206bc1

Browser Trust

Apple	Browser Trusted
Microsoft	Browser Trusted
Mozilla NSS	Browser Trusted

Key Usage and Constraints

Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Client Auth, Server Auth

Figure 7 – Certificate corroboration from Censys

The certificate structure for sellview[.]xyz is similar in structure to the original certificate for google247[.]xyz (from the SSLBL): the "Issuer DN" string is identical; validity period is 1 year, and the "Names" values are identically structured. There are now two domains with overlapping certificate characteristics being hosted on IP 14.241.72[.]25. Additional similarities can be seen within the WHOIS registration data: the registrant information was identical (Registrant Organization: Nguyễn Quang Thuỷ; Registrar: Mat Bao Corporation, and nameservers). Screenshots of both domains using URLSCAN.io also proved to be identical: a blank white screen with “Hello.” written in black text in the top-left corner {Figure 8}.

Hello

Figure 8 – Screenshot of the two domains

The matching WHOIS registration data, along with the identical certificate structure, hosting infrastructure, and URLSCAN website screenshots, indicate it is highly likely this activity can be clustered.

Next, PACT pivoted on the IP in an attempt to identify additional domains that might be clustered with the observed activity. Querying the IP using passive DNS and domain intelligence tools corroborated the hosting of the previously identified domains as well as dozens of other domains registered under the *.xyz TLD.

Some were immediately notable due to their similarity in name or theme:

1. google360[.]xyz
2. shippro[.]xyz
3. btc247[.]xyz
4. btc360[.]xyz
5. follow247[.]xyz
6. follow360[.]xyz
7. forex247[.]xyz
8. forex24h[.]xyz
9. gold247[.]xyz
10. gold360[.]xyz
11. googlevn[.]xyz
12. guess247[.]xyz
13. guess360[.]xyz
14. mailgoogle[.]xyz

Others appeared to target a Vietnamese-speaking audience:

1. Giaovat[.]xyz (translated*: “giao vat” = delivery)

2. Timviec[.]xyz (translated*: “tim viec” = heart)
3. Xemhang[.]vn (translated*: “xem hang” = see the cave)
4. Xemhang[.]xyz (see above)
5. Xuatban[.]xyz (translated*: “xuat ban” = leave you)

*translation provided using Google Translate

The shared theme of the domains (technology, cryptocurrency, re-use of numbering schemes [e.g., btc247, gold247, guess247] and the consistent use of the “.xyz” TLD), as well as the shared hosting infrastructure (IP 14.241.72[.]25), along with the overlapping WHOIS data, is used to loosely cluster this activity.

All domains listed above (22 in total) share the following characteristics:

1. Hosted (currently or previously) on IP 14.241.72.25
2. Registrant Organization: Nguyễn Quang Thuỷ
3. Registrar: Mat Bao Corporation
4. Name Servers: NS1.MATBAO.COM & NS2.MATBAO.COM

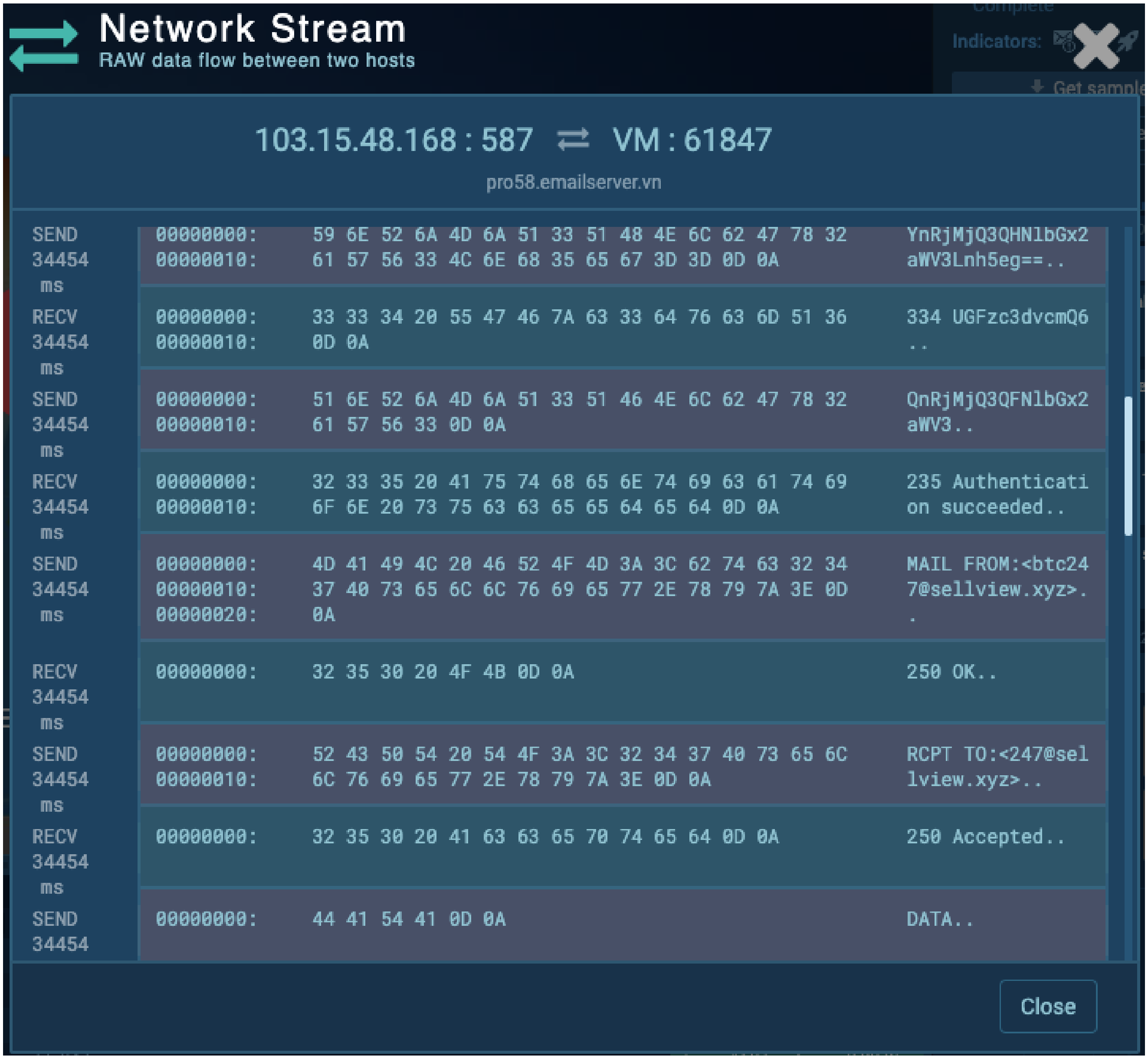
Additional Analysis

In keeping with the subject of this post, certificate analysis on all 22 domains continued strengthening the case for clustering this activity. 20 of the 22 domains have overlapping certificate characteristics: they were previously registered with 90-day certificates from Certificate Authority “ZeroSSL”, and 13 have a current 12-month certificate from Certificate Authority Sectigo. The Sectigo certificates share a common naming schema for the website/domain in the Common Name (CN) and Subject Alternative Names (SAN) as well as the ‘Issuer DN’ string “C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA”. Both the Sectigo and ZeroSSL certificates share the same naming schema in the CN and SAN fields.

Certificate histories were available for some of the domains as far back as 2016, which also revealed that this actor has been using multiple certificate authorities (Sectigo/Comodo, ZeroSSL, Let’s Encrypt). Expired certificates for some domains also revealed additional domains (via entries in the CN or SAN fields), but these domains were not included in the findings as historical hosting data was not available. It appears from certificate timestamps that the actor was using the ZeroSSL certs in early 2021, then recertified their domains using Sectigo as the ZeroSSL certs began expiring. The most recent certifications have a period of validity beginning on 08 July 2021 (for both btc360[.]xyz and btc247[.]xyz), indicating that the actor is actively maintaining this infrastructure. The expired ZeroSSL certs are timestamped largely from early 2021, with most valid beginning dates clustered in March 2021. Certificate histories could be identified as far back as 2016 for a few select domains, but the actor appears to have begun building out the current cluster of infrastructure in mid-2020 (June/July).

In order to visualize current and potential connections, the indicators were loaded into VirusTotal Graph. VT Graph enabled analysts to further pivot on malicious samples downloaded from and communicating with the domains and hosting infrastructure, as well as identify URLs and sub-domains clustered with the identified domains.

Further analysis of the malware hosted within these domains reinforces the interconnectedness of the network. The identified samples relied heavily on scripting and LOLbins to establish persistence in the victim machine and communicate with the threat actor. Additional payloads and scripts were retrieved from btc247[.]xyz. Communication was made via SMTP from btc247[@]sellview[.]xyz to 247@sellview[.]xyz leveraging a mailserver at emailserver[.]vn, a large Vietnamese webmail provider. {Figure 9,10}



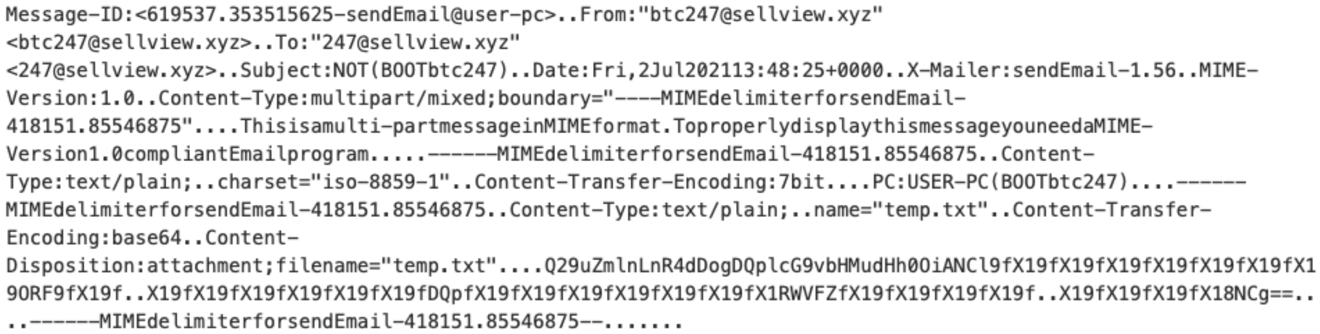
103.15.48.168 : 587 ⇄ VM : 61847

pro58.emailserver.vn

```
SEND   00000000:   59 6E 52 6A 4D 6A 51 33 51 48 4E 6C 62 47 78 32   YnRjMjQ3QHNlbGx2
34454  00000010:   61 57 56 33 4C 6E 68 35 65 67 3D 3D 0D 0A         aWV3Lnh5eg==..
 ms
RECV   00000000:   33 33 34 20 55 47 46 7A 63 33 64 76 63 6D 51 36   334 UGFzc3dvcmQ6
34454  00000010:   0D 0A                                             ..
 ms
SEND   00000000:   51 6E 52 6A 4D 6A 51 33 51 46 4E 6C 62 47 78 32   QnRjMjQ3QFNlbGx2
34454  00000010:   61 57 56 33 0D 0A                                 aWV3..
 ms
RECV   00000000:   32 33 35 20 41 75 74 68 65 6E 74 69 63 61 74 69   235 Authenticati
34454  00000010:   6F 6E 20 73 75 63 63 65 65 64 65 64 0D 0A         on succeeded..
 ms
SEND   00000000:   4D 41 49 4C 20 46 52 4F 4D 3A 3C 62 74 63 32 34   MAIL FROM:<btc24
34454  00000010:   37 40 73 65 6C 6C 76 69 65 77 2E 78 79 7A 3E 0D   7@sellview.xyz>.
 ms    00000020:   0A                                                .

RECV   00000000:   32 35 30 20 4F 4B 0D 0A                           250 OK..
34454
 ms
SEND   00000000:   52 43 50 54 20 54 4F 3A 3C 32 34 37 40 73 65 6C   RCPT TO:<247@sel
34454  00000010:   6C 76 69 65 77 2E 78 79 7A 3E 0D 0A               lview.xyz>..
 ms
RECV   00000000:   32 35 30 20 41 63 63 65 70 74 65 64 0D 0A         250 Accepted..
34454
 ms
SEND   00000000:   44 41 54 41 0D 0A                                 DATA..
34454
```

Figure 9 – Network traffic generated by infection



```
Message-ID:<619537.353515625-sendEmail@user-pc>..From:"btc247@sellview.xyz"
<btc247@sellview.xyz>..To:"247@sellview.xyz"
<247@sellview.xyz>..Subject:NOT(BOOTbtc247)..Date:Fri,2Jul202113:48:25+0000..X-Mailer:sendEmail-1.56..MIME-
Version:1.0..Content-Type:multipart/mixed;boundary="----MIMEdelimiterforsendEmail-
418151.85546875"....Thisisamulti-partmessageinMIMEformat.ToproperlydisplaythismessageyouneedaMIME-
Version1.0compliantEmailprogram.....------MIMEdelimiterforsendEmail-418151.85546875..Content-
Type:text/plain;..charset="iso-8859-1"..Content-Transfer-Encoding:7bit....PC:USER-PC(BOOTbtc247)....------
MIMEdelimiterforsendEmail-418151.85546875..Content-Type:text/plain;..name="temp.txt"..Content-Transfer-
Encoding:base64..Content-
Disposition:attachment;filename="temp.txt"....Q29uZmlnLnR4dDogDQplcG9vbHMudHh0OiANCl9fX19fX19fX19fX19fX19fX1
9ORF9fX19f..X19fX19fX19fX19fX19fX19fDQpfX19fX19fX19fX19fX19fX19fX1RWVFZfX19fX19fX19fX19f..X19fX19fX19fX18NCg==..
..------MIMEdelimiterforsendEmail-418151.85546875--.......
```

Figure 10 – SMTP communication from victim machine

The email attachment contains information from the victim machine indicating if it has a configuration file for TeamViewer or a specific cryptominer. Samples of this cryptominer were found in an open directory on one of the domains in this network. AeroAdmin is installed for remote control of the victim machine, but we were unable to link the AeroAdmin account back to any specific group or actor at this time.

Conclusion

Redaction of registration data previously available via WHOIS has left Threat Researchers and Threat Intel Analysts with a gap that can be bridged by investigation and clustering of TLS Certificates to identify adversary infrastructure. Thanks to the push for Certificate Transparency{12,13}, each CA continuously updates a permanent, append-only record of all certificates that have been associated to domains, which can then be leveraged to identify hosting infrastructure (and even adversary TTPs) by searching the data provided by the good folks doing the public service of scanning the internet {14}. Researchers hunting malicious infrastructure can continue to ply their trade while society grapples with GDPR and privacy law.

Notes on Analytical Gaps:

1. Prevailion Analysts do not currently possess region-specific, nuanced knowledge of the Vietnamese internet hosting market, so something like the choices of registrar may be restricted enough that multiple entities might be forced to use the same registrar and name server (leading to false confidence in clustering activity).
2. Long term hosting data (SSL certificate scans or pDNS data) may have enabled further pivot opportunities based upon domains observed in expired certificates.

REFERENCES:

1. https://medium.com/@mark.parsons/hunting-a-tls-certificate-series-post-1-6ad7adfebe44
2. [Mark Parsons @ SANS DFIR: Hunting Cyber Threat Actors with TLS Certificates] (https://www.youtube.com/watch?v=SieSrv8RGic)
3. [Ryan Kovar @ SANS DFIR:](https://www.youtube.com/watch?v=QA5OTUVqJiw)

4. https://www.riskiq.com/blog/external-threat-management/threat-hunting-post-whois/
5. https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects?utm_campaign=current-events-to-widespread-campaigns-pivoting-from-samples-to-identify&utm_source=Blog
6. https://osintcurio.us/2019/03/12/certificates-the-osint-gift-that-keeps-on-giving/
7. https://threatconnect.com/blog/infrastructure-research-hunting/
8. https://threatconnect.com/blog/track-to-the-future/
9. https://threatconnect.com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/
10. https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate
11. https://sslbl.abuse.ch/
12. https://www.rapid7.com/blog/post/2018/01/04/certificate-transparency-the-gift-that-keeps-giving/
13. https://transparencyreport.google.com/https/certificates?hl=en
14. https://scans.io/