Cyber Threat Intelligence Network, Inc.
P.O. Box 5042 | Carefree, AZ 85377 | USA
001 (928) 399-0509

OASIS Automation Workshop

Fileless and Socketless Backdoor Use Case: SockDetour

TiltedTemple Threat Actor[i]

R. Jane Ginn, MSIA
May 22, 2022
TLP=White

USE CASE TYPE: Mid-Level Scenario & Interoperability Demo

Introduction

Following is a curated Use Case built to meet the needs of the June 2, 2022, OASIS Automation Workshop for demonstrating interoperability of multiple security standards including:

- OpenC2
- Collaborative Automated Course of Action Operations (CACAO)
- Threat Actor Context (TAC)
- Cyber Threat Intelligence (CTI) [for STIX2.1 & TAXII2.1]
- Common Security Advisory Framework (CSAF)
- Open Security Alliance

This Use Case is a compilation of data from multiple sources about an ongoing threat posed by a sophisticated advanced persistent threat (APT). I have used open-source data for documenting TTPs used by the threat actor(s) as a secondary source and then conducted threat hunts on their ongoing reported malicious infrastructure as a primary source.

For the purposes of this Automation Workshop, I have chosen specific offensive actions taken by the threat actor for illustrative purposes to meet the needs of the participants in the Automation Workshop. I have supplemented historical findings from multiple threat hunt teams with my own findings of ongoing campaigns by the profiled threat actor. For consistency I use the threat actor naming convention used by PaloAlto's Unit42 threat hunting team: TiltedTemple. Some of the TTPs described also correlate with the following named threat actors:

- Emissary Panda[ii]
- TG-3390[iii]

This Use Case is intended to provide sufficient data at the macro level for strategic planning and at the micro level for interoperability testing.

Introduction

On September 16, 2021, the US Cybersecurity and Infrastructure Seopcurity Agency (CISA) released an alert warning that advanced persistent threat (APT) actors were actively exploiting newly identified vulnerabilities in a self-service password management and single sign-on solution known as Zoho ManageEngine ADSelfService Plus (CVE-2021-40539).[iv] The alert explained that malicious actors were observed deploying a specific webshell and other techniques to maintain persistence in victim environments.

As early as September 17, 2021, a threat actor leveraged leased infrastructure in the United States to scan hundreds of vulnerable organizations across the Internet in an effort to identify and enumerate devices with this vulnerability. Subsequently, exploitation attempts began on September 22, 2021, and likely continued into early October. During that window, the actor successfully compromised at least nine global entities across the technology, defense, healthcare, energy, and education industries.

About SockDetour[v]

An analysis team from Unit 42 tracked the threat actor responsible for the scanning activity which they named **TiltedTemple.** In addition to the first vulnerability that triggered the scanning activity TiltedTemple exploited a Zoho ServiceDesk Plus vulnerability (CVE-2021-44077)[vi] in their subsequent campaigns. The threat actors involved used a variety of techniques to gain access to and establish persistence in compromised systems.

In conducting further analysis of this campaign, they identified another sophisticated tool being used to maintain persistence: **SockDetour**. A custom backdoor, SockDetour is designed to serve as a backup backdoor in case the primary one is removed. It operates filelessly and socketlessly on compromised Windows servers.

Analysts from Unit42 could not conclude whether TiltedTemple was a single or multiple threat actors. Based on their telemetry data and the analysis of the collected samples, they asserted that the threat actor behind SockDetour targeted U.S.-based defense contractors since at least July 2019.

They discovered evidence that SockDetour was delivered from an external FTP server to a U.S.-based defense contractor's Internet-facing Windows server on July 27, 2021. They did not find any additional SockDetour samples on public repositories, meaning that the backdoor successfully stayed under the radar for a long time. The FTP server that hosted SockDetour was a compromised Quality Network Appliance Provider (QNAP) small office and home office (SOHO) network-attached storage (NAS) server. The NAS server is known to have multiple vulnerabilities, including a remote code execution vulnerability, CVE-2021-28799.[vii] On April 22, QNAP released a security advisory to disclose a vulnerability within their Hybrid Backup Sync (HBS 3) software. This software provides backup, restoration and synchronization functions between local, remote and cloud storage spaces. The vulnerability has been confirmed as an improper authorization vulnerability. Once exploited, it allows remote attackers to log in to the devices.

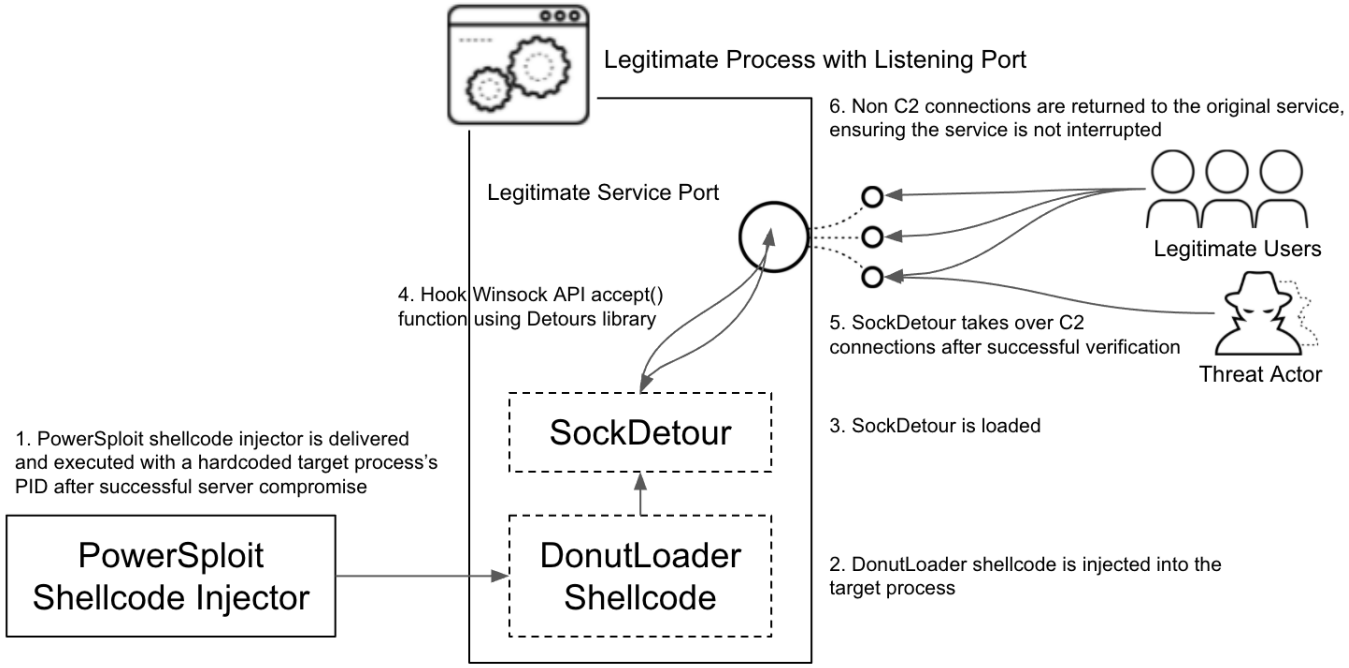
This QNAP vulnerability was leveraged by various ransomware families in massive infection campaigns in April 2021. The Unit42 researchers asserted that the TiltedTemple threat actor behind SockDetour likely also leveraged these vulnerabilities to compromise the NAS server.

Analysis of SockDetour

SockDetour is a custom backdoor compiled in 64-bit PE file format. It is designed to serve as a backup backdoor in case the primary one is detected and removed. It works on Windows operating systems that are running services with listening TCP ports. It hijacks network connections made to the pre-existing network socket and establishes an encrypted C2 channel with the remote threat actor via the socket. Thus, SockDetour requires neither opening a listening port from which to receive a connection nor calling out to an external network to establish a remote C2

channel. This makes the backdoor more difficult to detect from both host and network level.

In order for SockDetour to hijack an existing process's socket, it needs to be injected into the process's memory. For this reason, the threat actor converted SockDetour into a shellcode using an open source shellcode generator called Donut framework, then used the PowerSploit memory injector to inject the shellcode into target processes. The samples found contained hardcoded target processes' IDs, which means the threat actor manually chose injection target processes from compromised servers.



After SockDetour is injected into the target process, the backdoor leverages the Microsoft Detours library package, which is designed for the monitoring and instrumentation of API calls on Windows to hijack a network socket. Using the DetourAttach() function, it attaches a hook to the Winsock accept() function. With the hook in place, when new connections are made to the service port and the Winsock accept() API function is invoked, the call to the accept() function is re-routed to the malicious detour function defined in SockDetour.

Other non-C2 traffic is returned to the original service process to ensure the targeted service operates normally without interference. With such implementation, SockDetour is able to operate filelessly and socketlessly in compromised Windows servers, and serves as a backup backdoor in case the primary backdoor is detected and removed by defenders.

Client Authentication and C2 Communication

As SockDetour hijacks all the connections made to the legitimate service port, it first needs to verify the C2 traffic from incoming traffic that is mixed with legitimate service traffic, then authenticate to make sure the C2 connection is made from the right client.

SockDetour achieves the verification and authentication of the C2 connection with the following steps.

1. First, expect to receive 137 bytes of data from a client for authentication. The authentication data is as shown in the structure in Table 1.

17 03 03	AA BB	CC DD EE FF	128-byte data block
Fixed header value to disguise TLS traffic	Payload data size	Four-byte variable used for client authentication	Data signature for client authentication data block

Table 1. SockDetour client authentication data structure.

2. Read the first nine bytes of data. This data is received using the recv() function with the MSG_PEEK option so that it will not interfere with the legitimate service's traffic by removing data from the socket queue.

3. Verify that the data starts with 17 03 03, which is commonly seen as a record header for TLS transactions when encrypted data is being transferred. However, this is abnormal for normal TLS – a TLS-encrypted transaction would not normally show up without proper TLS handshakes.

```
.text:000007FEFAB84823 ; ---------------------------------------------------------------------------
.text:000007FEFAB84823
.text:000007FEFAB84823 loc_7FEFAB84823:                        ; CODE XREF: _hookingFunc+87↑j
.text:000007FEFAB84823                  mov     r9d, MSG_PEEK   ; flags
.text:000007FEFAB84829                  mov     r8d, 9          ; len
.text:000007FEFAB8482F                  lea     rdx, [rsp+218h+_RecvBuf] ; buf
.text:000007FEFAB84837                  mov     rcx, [rsp+218h+s] ; s
.text:000007FEFAB8483C                  call    cs:recv         ; recv 9 bytes
.text:000007FEFAB84842                  mov     [rsp+218h+Buf2], 17h
.text:000007FEFAB84847                  mov     [rsp+218h+var_1D3], 3
.text:000007FEFAB8484C                  mov     [rsp+218h+var_1D2], 3
.text:000007FEFAB84851                  mov     r8d, 3          ; Size
.text:000007FEFAB84857                  lea     rdx, [rsp+218h+Buf2] ; Buf2
.text:000007FEFAB8485C                  lea     rcx, [rsp+218h+_RecvBuf] ; Buf1
.text:000007FEFAB84864                  call    memcmp          ; data should start with 17 03 03
.text:000007FEFAB84869                  test    eax, eax
```

Figure 2. SockDetour receives data with the MSG_PEEK option and verifies the data.

4. Check that the size of payload data AA BB is less than or equal to 251.

5. Check that the four bytes of payload CC DD EE FF satisfy the conditions below:

   a. The result is 88 a0 90 82 after bitwise AND with 88 a0 90 82

   b. The result is fd f5 fb ef after bitwise OR with fd f5 fb ef

6. Read the whole 137 bytes of data from the same data queue with the MSG_PEEK option for further authentication.
7. Build a 24-byte data block as shown in Table 2.

08 1c c1 78 d4 13 3a d7 0f ab	CC DD EE FF	b3 a2 b8 ae 63 bb 03 e8 ff 3b
10 bytes hardcoded in SockDetour	Four bytes received from the client for authentication	10 bytes hardcoded in SockDetour

Table 2. 24-byte data block to be verified for client authentication.

8. This 24-byte data block is hashed and verified using an embedded public key against the 128-byte data signature in Table 1, which the threat actor would have created by signing the hash of the same 24-byte data

block using the corresponding private key. This completes the client authentication step. After successful authentication, SockDetour takes over the TCP session using the recv() function without the MSG_PEEK option as this session is now verified to be for the backdoor.

Next, SockDetour creates a 160-bit session key using a hardcoded initial vector value bvyiafszmkjsmqgl, then sends it to the remote client using the following data structure. In common encryption protocols such as TLS, the session key is encrypted with a public key before transferring. However, in this case, the malware author has seemingly forgotten the step and transfers the key in plain text.

`17 03 03`	`AA BB`	`CC DD EE FF`	`session_key`	`random_padding`
Fixed header value to disguise TLS traffic	Payload data size	Session key length	160-bit session key	Random padding

Table 3. SockDetour sending session key to client.

Now with the session key shared between SockDetour and the remote client, the C2 connection is made encrypted over the hijacked socket.

Plugin Loading Feature

As a backup backdoor, SockDetour serves only one feature of loading a plugin DLL. After the session key sharing, SockDetour receives four bytes of data from the client, which indicates the length of data SockDetour will receive for the final payload delivery stage. The size is expected to be smaller or equal to five MB.

The final payload data received is encrypted using the shared session key. After decryption, the received data is expected to be in JSON format with two objects app and args. app contains a base 64-encoded DLL, and args contains an argument to be passed to the DLL. SockDetour loads this plugin DLL in newly allocated memory space, then calls an export function with the name ThreadProc with a function argument in the following JSON structure.

```
{
    "sock": hijacked_socket,
    "key": session_key,
    "args": arguments_received_from_client
}
```

While plugin DLL samples were not discovered, the above function argument suggests that the plugin also likely communicates via the hijacked socket and encrypts the transaction using the session key. Thus, it likely operates as stealthily as SockDetour does.

Subsequent research by the Unit42 team provides more detail on other malware components used by the TiltedTemple threat actor that could also be used for interoperability testing.[viii] The Yara Rule for detecting SockDetour in memory is given as Appendix A.

MITRE ATT&CK Framework TTPs

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques (TTPs) based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The Unit42 researchers shared the ATT&CK Enterprise TTPs from the SockDetour campaign with the broader research community as STIX 2.1 patterning language properties encoded in Indicator STIX Domain Objects (SDOs) formatted as JSON objects. It is shared through the Atoms finder at: https://unit42.paloaltonetworks.com/atoms/tiltedtemple/ [See the 3rd tab labeled for the campaign that ran from September 2021 to September 2021].

The following screenshots provide values for several of the key ATT&CK Framework phases observed from the SockDetour campaign. Readers may cut-and-paste the Indicator Patterning Language code snippets directly from the strings given in the Atom tool [URL given above]. The following screenshots are illustrative of the type of information that can be used for Use Case interoperability demonstrations.

Persistence Phase – Web Shell

T1505.003: Web Shell Reference | **Courses of Actions**

Description	Indicator Pattern
Godzilla webshell	[file:hashes.'SHA-256' = '5475aec3b9837b514367c89d8362a9d524bfa02e75b85b401025588839a40bcb']
Godzilla webshell	[file:hashes.'SHA-256' = '75574959bbdad4b4ac7b16906cd8f1fd855d2a7df8e63905ab18540e2d6f1600']
Godzilla webshell	[file:hashes.'SHA-256' = 'a44a5e8e65266611d5845d88b43c9e4a9d84fe074fd18f48b50fb837fa6e429d']
Godzilla webshell	[file:hashes.'SHA-256' = 'ce310ab611895db1767877bd1f635ee3c4350d6e17ea28f8d100313f62b87382']

Privilege Escalation – Registry Run Keys/Startup Folder

T1547.001: Registry Run Keys / Startup Folder Reference | **Courses of Actions**

Description	Indicator Pattern
NGLite registry persistence KDC Service	[windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\KDC Service : regsvr32 /s user64.dll']
NGLite registry persistence Audit	[windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\ME_ADAudit.exe']
NGLite registry persistence ADManager	[windows-registry-key:key = 'HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\ME_ADManager.exe']

Credential Access Phase – LSASS Memory

T1003.001: LSASS Memory Reference | **Courses of Actions**

Description	Indicator Pattern
KdcSponge	[file:hashes.'SHA-256' = '3c90df0e02cc9b1cf1a86f9d7e6f777366c5748bd3cf4070b49460b48b4d4090']
KdcSponge	[file:hashes.'SHA-256' = 'b4162f039172dcb85ca4b85c99dd77beb70743ffd2e6f9e0ba78531945577665']

Credential Access Phase – API Hooking

T1056.004: Credential API Hooking Reference	Courses of Actions

Description	Indicator Pattern
KdcSponge	[file:hashes.'SHA-256' = '3c90df0e02cc9b1cf1a86f9d7e6f777366c5748bd3cf4070b49460b48b4d4090']
KdcSponge	[file:hashes.'SHA-256' = 'b4162f039172dcb85ca4b85c99dd77beb70743ffd2e6f9e0ba78531945577665']

Command and Control – Web Protocols

T1071.001: Web Protocols Reference	Courses of Actions

Description	Indicator Pattern
Threat Actor IP Addresses	[ipv4-addr:value = '140.82.17.161']
Threat Actor IP Addresses	[ipv4-addr:value = '149.248.11.205']
Threat Actor IP Addresses	[ipv4-addr:value = '149.28.93.184']
Threat Actor IP Addresses	[ipv4-addr:value = '199.188.59.192']
Threat Actor IP Addresses	[ipv4-addr:value = '24.64.36.238']
Threat Actor IP Addresses	[ipv4-addr:value = '45.63.62.109']
Threat Actor IP Addresses	[ipv4-addr:value = '45.76.173.103']
Threat Actor IP Addresses	[ipv4-addr:value = '45.77.121.232']
Threat Actor IP Addresses	[ipv4-addr:value = '66.42.98.156']

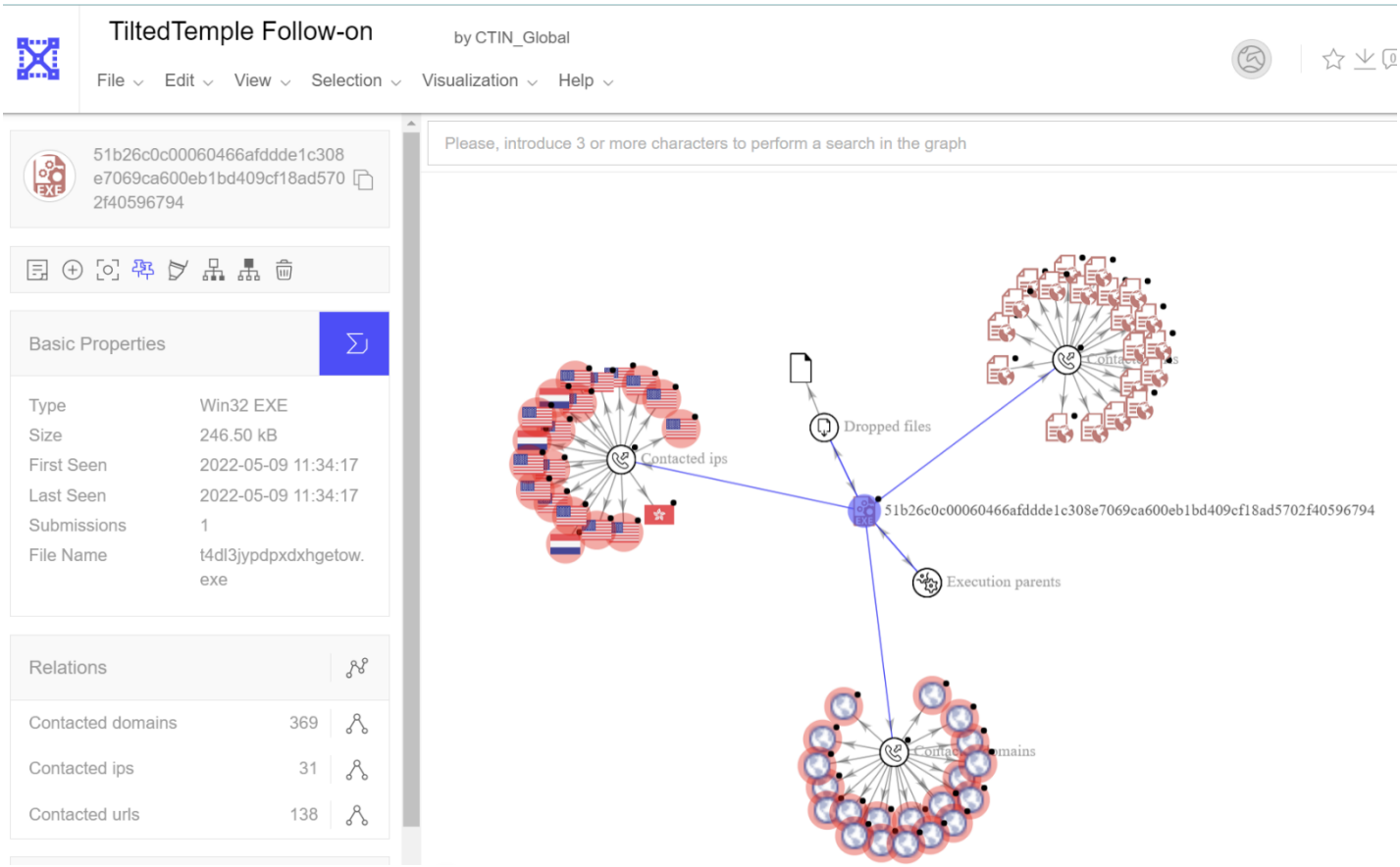
Command and Control – Ingress Tool Transfer

T1105: Ingress Tool Transfer Reference	Courses of Actions

Description	Indicator Pattern
NGLite	[file:hashes.'SHA-256' = '3da8d1bfb8192f43cf5d9247035aa4445381d2d26bed981662e3db34824c71fd']
NGLite	[file:hashes.'SHA-256' = '3f868ac52916ebb6f6186ac20b20903f63bc8e9c460e2418f2b032a207d8f21d']
NGLite	[file:hashes.'SHA-256' = '5b8c307c424e777972c0fa1322844d4d04e9eb200fe9532644888c4b6386d755']
Godzilla Webshell and NGLite dropper	[file:hashes.'SHA-256' = '5fcc9f3b514b853e8e9077ed4940538aba7b3044edbba28ca92ed37199292058']
NGLite	[file:hashes.'SHA-256' = '805b92787ca7833eef5e61e2df1310e4b6544955e812e60b5f834f904623fd9f']
Godzilla Webshell and NGLite dropper	[file:hashes.'SHA-256' = 'b2a29d99a1657140f4e254221d8666a736160ce960d06557778318e0d1b7423b']

Current Campaign

As noted above, this campaign is ongoing. I have conducted research on Cyber Observables (COs) published by CISA, Unit42 and other into the ongoing campaigns of TiltedTemple and or affiliated threat actors using the same TTPs and/or malicious infrastructure. An investigation into a single Cyber Observable from the above research (140.82.17[.]161) showed me that the malicious infrastructure described by Unit42 is still being used by either the TiltedTemple threat actor or an affiliated group. By selecting one of the most recent executables (t4dl3jypdpxdxhgetow[.]exe) (SHA256: 51b26c0c00060466afddde1c308e7069ca600eb1bd409cf18ad5702f40596794) from the currently active data set I was able to generate the following graph on VirusTotal:

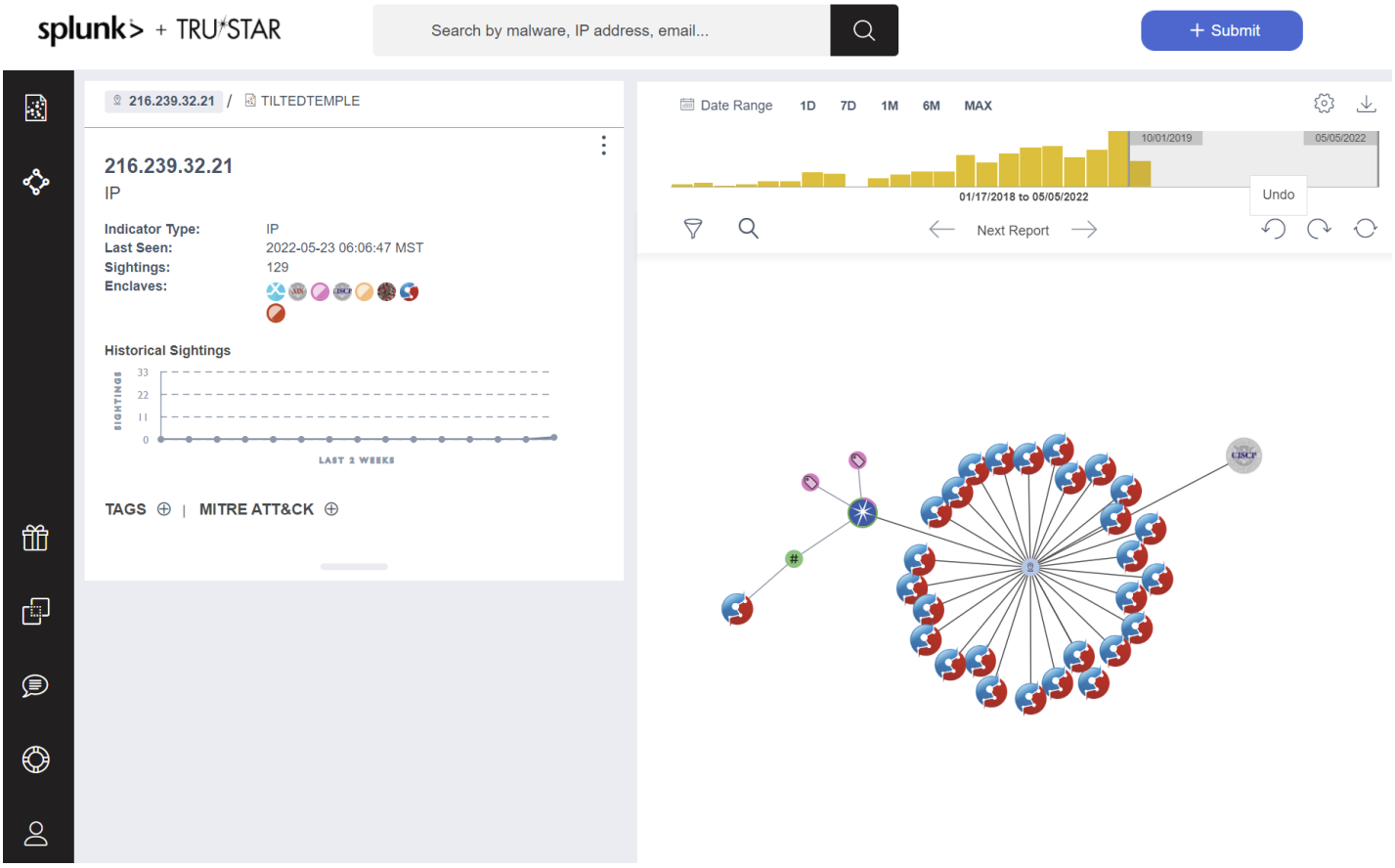


By following just one of the IPv4 values given in the Web Protocols image I was able to surface an ongoing malware campaign associated with the TiltedTemple malicious infrastructure. A list of the MD5 malware hashes from this current campaign is given as Appendix B to this Use Case description.[ix]

The IPv4 address 216.239.32[.]21 appears to be the most active IP disseminating emails in ongoing phishing campaigns. It is a Google name server with a pointer record 'any-in2015.1e100.net' on AS15169. QratorLabs has identified 549,200 vulnerable ports, 827 hijacks, 4 route leaks and 1,769 DDoS Amplifiers in this autonomous system.

An analysis of pDNS data shows that the currently active phishing campaign correlates to activity observed on the Georgia Tech labs bare metal servers as recently as May 5, 2022, from multiple domains. Details are given in Appendix B. This IPv4 also correlates to a set of malware on VirusTotal from 2018. These data are given as Appendix C.

A TRUSTAR run on the full set of data from Appendix B provides the following graph:



The correlation of the current campaign with the 2018 and 2019 campaigns can be seen from the timeline above the graph with extensive activity beginning in 2018 as corroborated by the VirusTotal malware hashes given in Appendix C. This more recent campaign appears to be using this older malicious infrastructure. The node at the center of the circle of the blue and red HybridAnalysis nodes is 216.239.32[.]21. This image illustrates the centrality of that IP address in the current, ongoing phishing campaign.

Conclusions

SockDetour is a backdoor that is designed to remain stealthily on compromised Windows servers so that it can serve as a backup backdoor in case the primary one fails. It is filelessly loaded in legitimate service processes and uses legitimate processes' network sockets to establish its own encrypted C2 channel. According to Unit42 it has likely been in the wild since at least July 2019 without any update to the PE file.

The plugin DLL described above remains unknown, but it is also expected to operate very stealthily by being delivered via the SockDetour's encrypted channel, being loaded filelessly in memory and communicating via hijacked sockets. As an additional note, the type of NAS server found hosting SockDetour is typically used by small businesses, hence the SOHO designation.

It is unknown at this time whether or not the current phishing campaign is distributing the SockDetour malware; however, given the overlapping infrastructure and the history of TiltedTemple, it is a possibility. The Yara Rule given in Appendix A will help defenders detect its presence on a network.

Appendix A – Yara Rule for Detecting SockDetour in Memory

```
rule apt_win_sockdetour
{
	meta:
		author = "Unit 42 - PaloAltoNetworks"
		date = "2022-01-23"
		description = "Detects SockDetour in memory or in PE format"
		hash01 = "0b2b9a2ac4bff81847b332af18a8e0705075166a137ab248e4d9b5cbd8b960df"
	strings:
		$public_key =
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWD9BUhQQZkagIIHsCdn/wtRNXcYoEi3Z4PhZkH3mar20EONVyX
WP/YUxyUmxD+aTOVp3NB+XYOO9LqQEAWgyGndXyyuDssLWTb7z54n8iDu2pqiAEvJ6h18iwf0EwZ1BzPBDS1Kw+JE4tYI
R860rD1DBul0u6OURqMPb5eZT1bQIDAQAB"
		$json_name_sequence = {61 70 70 00 61 72 67 73 00 00 00 00 73 6F 63 6B 00 00 00 00 6B 65 79 00 61
72 67 73 00 00}
		$verification_bytes = {88 [4] A0 [4] 90 [4] 82 [4] FD [4] F5 [4] FB [4] EF}
		$data_block = {08 [4] 1C [4] C1 [4] 78 [4] D4 [4] 13 [4] 3A [4] D7 [4] 0F [4] AB [4] B3 [4] A2 [4] B8 [4] AE
[4] 63 [4] BB [4] 03 [4] E8 [4] FF [4] 3B}
		$initial_vector = {62 [4] 76 [4] 79 [4] 69 [4] 61 [4] 66 [4] 73 [4] 7A [4] 6D [4] 6B [4] 6A [4] 73 [4] 6D [4]
71 [4] 67 [4] 6C}
	condition:
		any of them
}
rule apt_win_sockdetour
{
	meta:
		author = "Unit 42 - PaloAltoNetworks"
		date = "2022-01-23"
		description = "Detects SockDetour in memory or in PE format"
		hash01 = "0b2b9a2ac4bff81847b332af18a8e0705075166a137ab248e4d9b5cbd8b960df"
	strings:
		$public_key =
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWD9BUhQQZkagIIHsCdn/wtRNXcYoEi3Z4PhZkH3mar20EONVyX
WP/YUxyUmxD+aTOVp3NB+XYOO9LqQEAWgyGndXyyuDssLWTb7z54n8iDu2pqiAEvJ6h18iwf0EwZ1BzPBDS1Kw+JE4tYI
R860rD1DBul0u6OURqMPb5eZT1bQIDAQAB"
		$json_name_sequence = {61 70 70 00 61 72 67 73 00 00 00 00 73 6F 63 6B 00 00 00 00 6B 65 79 00 61
72 67 73 00 00}
		$verification_bytes = {88 [4] A0 [4] 90 [4] 82 [4] FD [4] F5 [4] FB [4] EF}
		$data_block = {08 [4] 1C [4] C1 [4] 78 [4] D4 [4] 13 [4] 3A [4] D7 [4] 0F [4] AB [4] B3 [4] A2 [4] B8 [4] AE
[4] 63 [4] BB [4] 03 [4] E8 [4] FF [4] 3B}
		$initial_vector = {62 [4] 76 [4] 79 [4] 69 [4] 61 [4] 66 [4] 73 [4] 7A [4] 6D [4] 6B [4] 6A [4] 73 [4] 6D [4]
71 [4] 67 [4] 6C}
	condition:
		any of them
}
```

Appendix B – Most Recent Campaign Using TiltedTemple Infrastructure

Cyber Observable Objects (SCOs)

Host Name	MD5 Hash Value	ipv4	UTC Timestamp
{"hname":"middleriver.net"	hash:"e08e81ead15950eb91b3cee966604c13"	ip:"216.239.32.21"	ts:"2022-05-11T23:59:59.000Z"
{"hname":"middleriver.net"	hash:"d678ff1fe2fdd44ff8a79c8e715105fe"	ip:"216.239.32.21"	ts:"2022-05-11T23:59:59.000Z"
{"hname":"tradehappen.net"	hash:"856a0ebb7c39ee7498156033ec97d890"	ip:"216.239.32.21"	ts:"2022-05-09T23:59:59.000Z"
{"hname":"jemshr.com"	hash:"2b342fc962d2f0d547de2aa01eefbdc6"	ip:"216.239.32.21"	ts:"2022-05-05T23:59:59.000Z"
{"hname":"signalred.biz"	hash:"01d4ec89887c5fa56a29aaade5521ea4"	ip:"216.239.32.21"	ts:"2022-05-05T23:59:59.000Z"
{"hname":"pcebio.com"	hash:"3d88e476c49f7f972a3cab0b940243c0"	ip:"216.239.32.21"	ts:"2022-05-01T23:59:59.000Z"
{"hname":"srbovi.com"	hash:"c8a7f9e3819d725c0c5c6069027308d5"	ip:"216.239.32.21"	ts:"2022-04-30T23:59:59.000Z"
{"hname":"bolaap.com"	hash:"241892f100b9179d5af588ebe0bb0820"	ip:"216.239.32.21"	ts:"2022-04-29T23:59:59.000Z"
{"hname":"bolaap.com"	hash:"2706ef2488d58f5c098205bcc4284770"	ip:"216.239.32.21"	ts:"2022-04-29T23:59:59.000Z"
{"hname":"cfpwyo.com"	hash:"226cb528b1d6e613f8c4a51af7296070"	ip:"216.239.32.21"	ts:"2022-04-29T23:59:59.000Z"
{"hname":"yairoo.com"	hash:"177dad8a51d0cb7118450ca50dc5c9c5"	ip:"216.239.32.21"	ts:"2022-04-22T23:59:59.000Z"
{"hname":"greatartsales.com"	hash:"79120df83885646cba34a15b6c755f4f"	ip:"216.239.32.21"	ts:"2022-04-22T23:59:59.000Z"
{"hname":"orkut.com"	hash:"c5eff9c69209f06e40a5bb8731a2e098"	ip:"216.239.32.21"	ts:"2022-04-22T23:59:59.000Z"
{"hname":"greatartsales.com"	hash:"f39b26c2a8c2f2dde6a16a08d35ef5d7"	ip:"216.239.32.21"	ts:"2022-04-21T23:59:59.000Z"
{"hname":"offyon.com"	hash:"29d696839c7365ea254eca575a18ade2"	ip:"216.239.32.21"	ts:"2022-04-18T23:59:59.000Z"
{"hname":"actdes.com"	hash:"f6934e90b26c13b22f54f0242b62ece3"	ip:"216.239.32.21"	ts:"2022-04-16T23:59:59.000Z"
{"hname":"eagros.com"	hash:"617818e7a7ae6511973d522890056a83"	ip:"216.239.32.21"	ts:"2022-04-15T23:59:59.000Z"
{"hname":"eagros.com"	hash:"a7c10e85e879d1072c52647e061b8e58"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"6d93c66a2103827d6f27a88f9552ecdb"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"3c51b537468fe93f180f0ef6888a440b"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"21a2f612a7e4db43a7559f0ef04ea63b"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"4f1e1d4ff48ad0d5782752b315e68d6e"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"1fc20d2d33dff4c25eea71eb4f1a1db3"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"

{"hname":"captainapple.net"	hash:"2069422096c542e77324f4655ad70372"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"6dda6307f23801ba7c493f56e9f3684a"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"orkut.com"	hash:"18150e854cfcef0772797c6b1f7f9930"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"ustacp.com"	hash:"04441b647e1c59e640c681a653ee0f8f"	ip:"216.239.32.21"	ts:"2022-04-14T23:59:59.000Z"
{"hname":"captainapple.net"	hash:"e94cd7aae267474413cbfd82d301925d"	ip:"216.239.32.21"	ts:"2022-04-13T23:59:59.000Z"
{"hname":"oinavi.com"	hash:"ca4ee5c40183e54bb55f5dda801dab8d"	ip:"216.239.32.21"	ts:"2022-04-12T23:59:59.000Z"
{"hname":"orkut.com"	hash:"fb6410520c048dd38d2ce485b2a32e25"	ip:"216.239.32.21"	ts:"2022-04-07T23:59:59.000Z"
{"hname":"higecc.com"	hash:"c779630a74e86f63e92b06eb192abba7"	ip:"216.239.32.21"	ts:"2022-04-06T23:59:59.000Z"
{"hname":"cryrye.com"	hash:"f15a4ebab00dbb1c94f3452ef2c482cb"	ip:"216.239.32.21"	ts:"2022-03-28T23:59:59.000Z"
{"hname":"rishigangoly.com"	hash:"78a9986ffe37badedecced11a70330a6"	ip:"216.239.32.21"	ts:"2022-03-24T23:59:59.000Z"
{"hname":"texsec.com"	hash:"c796c47c42e33ab64499e59fa8e062b4"	ip:"216.239.32.21"	ts:"2022-03-23T23:59:59.000Z"
{"hname":"csainz.com"	hash:"bd243b7126828983b1c703c5910293a5"	ip:"216.239.32.21"	ts:"2022-03-22T23:59:59.000Z"
{"hname":"csainz.com"	hash:"bff1df035e2e11ba006966d6d2234621"	ip:"216.239.32.21"	ts:"2022-03-22T23:59:59.000Z"
{"hname":"opecme.com"	hash:"4663fe1e35b3bf03658939694e21231b"	ip:"216.239.32.21"	ts:"2022-03-21T23:59:59.000Z"
{"hname":"rishigangoly.com"	hash:"c580c2349435a1cefd5939fb9d27f5ab"	ip:"216.239.32.21"	ts:"2022-03-20T23:59:59.000Z"
{"hname":"giacoo.com"	hash:"de0661b245d9d0002289b224d573275a"	ip:"216.239.32.21"	ts:"2022-03-12T23:59:59.000Z"
{"hname":"giacoo.com"	hash:"b028e126cd399729b09da75d56a6448f"	ip:"216.239.32.21"	ts:"2022-03-12T23:59:59.000Z"
{"hname":"ronyca.com"	hash:"f59f01c184f6fec5590f1f0b9d716fa8"	ip:"216.239.32.21"	ts:"2022-03-11T23:59:59.000Z"
{"hname":"ketomealprep.academy"	hash:"0fd100bc752335d0023893cc2104019a"	ip:"216.239.32.21"	ts:"2022-03-05T23:59:59.000Z"
{"hname":"electriccorner.net"	hash:"4bf7ae9fd16bcb146a6ec8de2be8a3b6"	ip:"216.239.32.21"	ts:"2022-02-25T23:59:59.000Z"
{"hname":"bdware.net"	hash:"84591a45462451816c8cf8078317734b"	ip:"216.239.32.21"	ts:"2022-02-09T23:59:59.000Z"
{"hname":"journeyfurther.net"	hash:"2bc773bf66c9e4efef1de93d5ba9e819"	ip:"216.239.32.21"	ts:"2022-02-08T23:59:59.000Z"
{"hname":"journeyfurther.net"	hash:"0c147b67318e95e757211a82f359c682"	ip:"216.239.32.21"	ts:"2022-02-07T23:59:59.000Z"
{"hname":"soitiz.com"	hash:"864f1b5e2a6fea9263a61f89fb70bfaa"	ip:"216.239.32.21"	ts:"2022-02-06T23:59:59.000Z"
{"hname":"heyhae.com"	hash:"8ae1674a8cf06bbfc6679b72e73f6452"	ip:"216.239.32.21"	ts:"2022-02-06T23:59:59.000Z"
{"hname":"iffxiv.com"	hash:"0a7938e26a0fcf842492ed585010ab2d"	ip:"216.239.32.21"	ts:"2022-02-03T23:59:59.000Z"
{"hname":"tkand.com"	hash:"fc0a044d291ed253d001d791f22aeee3"	ip:"216.239.32.21"	ts:"2022-01-28T23:59:59.000Z"
{"hname":"sites.simbla.com"	hash:"ab902acb5106f7d96d8cb95bb162e37c"	ip:"216.239.32.21"	ts:"2022-01-16T23:59:59.000Z"

{"hname":"sites.simbla.com"	hash:"4a317d17b5afc44656415e587b6bd25f"	ip:"216.239.32.21"	ts:"2022-01-16T23:59:59.000Z"
{"hname":"umacco.com"	hash:"ad612d4089f0c35cb6ae971194b91c0f"	ip:"216.239.32.21"	ts:"2022-01-06T23:59:59.000Z"
{"hname":"stlawrencecatholicschool.com"	hash:"03118223ded5ae14700b3b08fcf1600b"	ip:"216.239.32.21"	ts:"2022-01-05T23:59:59.000Z"
{"hname":"weebee.com"	hash:"c05fbd2028ab7833df0bfe7d1e4933ec"	ip:"216.239.32.21"	ts:"2022-01-05T23:59:59.000Z"
{"hname":"wepaintremodel.com"	hash:"4318cd03b349bc4b9ec123875d8da829"	ip:"216.239.32.21"	ts:"2022-01-05T23:59:59.000Z"
{"hname":"weebee.com"	hash:"9da0ea8d39d4958cf31b65a1fe42e5dd"	ip:"216.239.32.21"	ts:"2022-01-05T23:59:59.000Z"
{"hname":"simpleoffice.net"	hash:"3b2b70b8915dc490bc91c194b0c3ec69"	ip:"216.239.32.21"	ts:"2022-01-04T23:59:59.000Z"
{"hname":"voloch.com"	hash:"3934e5a8a594b9ad6e3a4f011e64daf6"	ip:"216.239.32.21"	ts:"2022-01-03T23:59:59.000Z"
{"hname":"voloch.com"	hash:"378cde7a0baf80a27330df708f9dac70"	ip:"216.239.32.21"	ts:"2022-01-03T23:59:59.000Z"
{"hname":"oobmab.com"	hash:"4cf4baae2495d90c10f052b0682bac1e"	ip:"216.239.32.21"	ts:"2022-01-02T23:59:59.000Z"
{"hname":"voloch.com"	hash:"e0105424bf4b6e38bb1c5386b2bb224a"	ip:"216.239.32.21"	ts:"2022-01-02T23:59:59.000Z"
{"hname":"eumcnc.com"	hash:"f5be122cce3a044abaada9ed58b653ca"	ip:"216.239.32.21"	ts:"2021-12-30T23:59:59.000Z"
{"hname":"eumcnc.com"	hash:"aa61945c1d5a39e484ad5192a040a0a2"	ip:"216.239.32.21"	ts:"2021-12-30T23:59:59.000Z"
{"hname":"iscria.com"	hash:"62829c5448a13de62197417b99c074f4"	ip:"216.239.32.21"	ts:"2021-12-29T23:59:59.000Z"
{"hname":"drewot.com"	hash:"c9ff2ff04a75f3867ad5ceeddd07cae5"	ip:"216.239.32.21"	ts:"2021-12-26T23:59:59.000Z"
{"hname":"drewot.com"	hash:"5dfe28cdb8551c26e4c4e2c962848851"	ip:"216.239.32.21"	ts:"2021-12-26T23:59:59.000Z"
{"hname":"sites.simbla.com"	hash:"75776701e1c9389a4890bdab8821b3bb"	ip:"216.239.32.21"	ts:"2021-12-25T23:59:59.000Z"
{"hname":"sites.simbla.com"	hash:"19bb607d85547fab8ed546fa10e9c29b"	ip:"216.239.32.21"	ts:"2021-12-25T23:59:59.000Z"
{"hname":"sites.simbla.com"	hash:"631afa73902cbc01164607d704d5cc32"	ip:"216.239.32.21"	ts:"2021-12-25T23:59:59.000Z"
{"hname":"sites.simbla.com"	hash:"d113fd876095bf230236e7b35b95c10b"	ip:"216.239.32.21"	ts:"2021-12-19T23:59:59.000Z"
{"hname":"partyready.net"	hash:"3832104361839b5217be023acdd23622"	ip:"216.239.32.21"	ts:"2021-12-14T23:59:59.000Z"
{"hname":"partyready.net"	hash:"395d63bc96728721fdcb42de23258c6c"	ip:"216.239.32.21"	ts:"2021-12-14T23:59:59.000Z"
{"hname":"caizou.com"	hash:"1f8b68b7e262644e0388fa32f57842fd"	ip:"216.239.32.21"	ts:"2021-12-10T23:59:59.000Z"
{"hname":"ketomealprep.academy"	hash:"956274df4e08be7860ebb9fbf4a75930"	ip:"216.239.32.21"	ts:"2021-11-13T23:59:59.000Z"
{"hname":"kincza.com"	hash:"060faad71961be4e9ce475ca772b508e"	ip:"216.239.32.21"	ts:"2021-11-07T23:59:59.000Z"
{"hname":"midwestschool.org"	hash:"53be606af2e57ed5911f838783a3f20e"	ip:"216.239.32.21"	ts:"2021-11-05T23:59:59.000Z"
{"hname":"rishigangoly.com"	hash:"d847056c86635f2041ac6be60e02b4b2"	ip:"216.239.32.21"	ts:"2021-11-05T23:59:59.000Z"
{"hname":"rishigangoly.com"	hash:"53be606af2e57ed5911f838783a3f20e"	ip:"216.239.32.21"	ts:"2021-11-05T23:59:59.000Z"

{"hname":"rishigangoly.com"	hash:"5726ab069063b51b8f24e78da4b9f42e"	ip:"216.239.32.21"	ts:"2021-11-05T23:59:59.000Z"
{"hname":"ketomealprep.academy"	hash:"7d7ee58c2696794b3be958b165eb61a9"	ip:"216.239.32.21"	ts:"2021-11-05T23:59:59.000Z"
{"hname":"resultcompany.net"	hash:"36dd328a1a8cb4d8d34d555ed3550369"	ip:"216.239.32.21"	ts:"2021-11-03T23:59:59.000Z"
{"hname":"rishigangoly.com"	hash:"f1bb4ac9fbf0f3f153826069aa4c0281"	ip:"216.239.32.21"	ts:"2021-10-31T23:59:59.000Z"
{"hname":"gegira.com"	hash:"1ef953227c3859ce430fb1d7ac24c859"	ip:"216.239.32.21"	ts:"2021-10-28T23:59:59.000Z"
{"hname":"tradehappen.net"	hash:"9bbe52b2f8136dc557e762fc0a4f38bb"	ip:"216.239.32.21"	ts:"2021-10-27T23:59:59.000Z"
{"hname":"tradeshare.net"	hash:"5090d0092e9ca1103e11eee3cf15bac2"	ip:"216.239.32.21"	ts:"2021-10-27T23:59:59.000Z"
{"hname":"rixten.com"	hash:"056b316633cbf371b77ea65b68880b80"	ip:"216.239.32.21"	ts:"2021-10-27T23:59:59.000Z"
{"hname":"cianfu.com"	hash:"40f4860ac170c8a84b212383c60fd9bc"	ip:"216.239.32.21"	ts:"2021-10-27T23:59:59.000Z"
{"hname":"alyeyo.com"	hash:"510154d7078df0b676c0a401da7701f4"	ip:"216.239.32.21"	ts:"2021-10-26T23:59:59.000Z"
{"hname":"amberange.com"	hash:"41b595bdd60ed33d8cec162229212edc"	ip:"216.239.32.21"	ts:"2021-10-25T23:59:59.000Z"
{"hname":"joliao.com"	hash:"a4cac8f3d4fa47a5463b29ad59ecf795"	ip:"216.239.32.21"	ts:"2021-10-23T23:59:59.000Z"
{"hname":"tradevalue.net"	hash:"168bd43ed72d4f8dd5610cca8e9db9fd"	ip:"216.239.32.21"	ts:"2021-10-20T23:59:59.000Z"
{"hname":"afpshi.com"	hash:"e73a955cda2cdaf2a675c68cf7521c52"	ip:"216.239.32.21"	ts:"2021-10-17T23:59:59.000Z"
{"hname":"kakamo.com"	hash:"00a4ed90e271bce8d35c7fae63ab0eeb"	ip:"216.239.32.21"	ts:"2021-10-17T23:59:59.000Z"
{"hname":"afpshi.com"	hash:"2d80eadf87f270bf6645736ad3c00263"	ip:"216.239.32.21"	ts:"2021-10-16T23:59:59.000Z"
{"hname":"heavengarden.net"	hash:"2a14a075912ceff4574c27bd5898798c"	ip:"216.239.32.21"	ts:"2021-10-12T23:59:59.000Z"
{"hname":"heavengarden.net"	hash:"314597a839d808b52f0cfafbb4127d60"	ip:"216.239.32.21"	ts:"2021-10-12T23:59:59.000Z"
{"hname":"heavengarden.net"	hash:"fec927964b095762ee1c6de916a251b4"	ip:"216.239.32.21"	ts:"2021-10-12T23:59:59.000Z"
{"hname":"heavengarden.net"	hash:"0bac02b498af12986801cb0ddc975fae"	ip:"216.239.32.21"	ts:"2021-10-12T23:59:59.000Z"
{"hname":"heavengarden.net"	hash:"255250f11c13800b2209a3c1c5ca722c"	ip:"216.239.32.21"	ts:"2021-10-12T23:59:59.000Z"

Appendix C – VirusTotal Data – 2018 Campaign

Date and Time	Positives	Total	SHA256 Hashes
6/17/2018 2:41	43	67	96aaad117b132cd41b61af831c75f8871e6f0c9f05159e3aaf332e1a1c067eb8
6/17/2018 0:48	38	68	2527364ec9f649e8ef88d35e0e5a1b82d2b8151f31932a9a8ca41bb9be72d56d
6/16/2018 1:15	35	68	a99b30304194001f1396a8c3619dbf980fb8e0852bab0b90912f9b31f8ad8c7e
6/15/2018 12:31	35	67	99bc48cdfbad8515e614bf4569480814d13491cc89281be85dbe3d203197f10c
6/10/2018 17:53	19	68	db12e2a7c8e014b65ff954ebdbc62c8fc8b7fb82218e61ce9e063e05d2e84e49
6/10/2018 10:17	32	68	b654c2229940ec8c3c2ee9c1c02701e95473f1721b3387f0309dfc5dcc469ab5
6/8/2018 1:31	40	68	fecdfc9a7f99cc73bcab4fdcf00541e034bd26e82efe1b7c17d5f574e3487eb7

6/7/2018 15:33	61	68	0eaaf60febc725b30cbf745924bbe8acddc138bdbbfcae607d5d7740dca64267
6/5/2018 17:14	44	68	02dce70bd61ddcb2b00cd70096de5fe152afc1b313169149eaef38b484d2b1e6
6/5/2018 16:58	42	67	215b9401dd8a4c6bd96b4070f0c68e02263af4902b1fcdca4b5a95f6786c37b7
6/4/2018 11:25	20	65	a6f96dc32e1367c7822ce60cbf983bd58c3a4721b68d171504f312ecf7e9880f
6/2/2018 19:35	20	66	a932fdfa8e2ca58aea8b9f2505a6ccee59bddf574c42b50f15334b51ae426c37
6/1/2018 23:10	43	67	7549bfde5a46b4e1675c2eb69285a96cd4c14245938ca6940d4c30a43de0f247
6/1/2018 11:01	20	66	5bdda298b8e65e797da4790af6f7fa4c653013480a85380de4975dfb0b920d88
5/31/2018 1:45	40	64	43ece924e9c1b1c5136883eba974b57c223e3e178a2abdfff71ea8fc74ecaaa8
5/30/2018 19:38	36	66	beffd70fc9a8c22b03366c45c60b55e0a2e5cda89c79c613bf4358593ea6a68b
5/30/2018 15:11	34	66	ecce544e65345f63dcf87a186c084481ac80e4e3f010b9df55b75acbc5d0086a
5/29/2018 12:12	38	63	7c3dde675f89726a9391d5e613b64792f63bb8f711444ec8a4198a2ab871aab2
5/29/2018 6:08	46	66	fbbd58cc74dd0836d1d9271debbba241d1d5e123d7c15a48dd1e3c0cc4f0b967
5/29/2018 5:02	22	66	7159fd0495272b8865eef0100b137c04c8c6ca4fb23d5f4a1b63905446dc1565
5/27/2018 11:42	47	66	b2c6ac89f6de6d58e417930c420835b55999c14c72e4a3b5016aebbbde05954a
5/27/2018 8:52	42	64	dca8d4b5962c23c3a31a27964428abfe524232443a18041be04b72e8e60bdb6f
5/26/2018 23:12	24	65	4bba8582915b79e021c29b97e1baa4e06066812c1f3b04bcfd9ea4d49446e3ea
5/26/2018 18:53	23	66	d81f04dcb9adaaf2c51a66ebfec7b1a255537ceffc666b48ad9b5504351f3522
5/25/2018 22:39	39	66	dfd1f5e31ac7c251a315ca9a30f509f06a11bd4a56e7f349e2ffca4fef62e1f6
5/25/2018 21:19	38	66	6ff7a7a1e8dd211721e8a4b9a418c5de572d54b55853e80c436f73c4afc49f78
5/25/2018 20:50	38	65	a6925073618e9b269293ef76a348cea7543bbd436bce381e1f159dd6cb7d5920
5/25/2018 12:05	3	65	0664113dbaee2e0c5a4b5694ad47ffe873473c0f49971e18ad2278d552c5d290
5/25/2018 8:18	30	66	5de78689b216763ad691cf1434d5ff9787e17c0cc64b4eda2c72d825756beaa3
5/24/2018 16:25	37	65	dfb074eaac8b3b6365ed28b52fbdacee0aae65367bfd151d6d6f22f3b88ce957
5/24/2018 10:28	1	66	de57e907db23c142f99100f41e14fb36b09da2de3272cf42887565c8b33e7197
5/24/2018 2:07	25	66	88525bae7cd17161edcb9f5dd08f24ac3772613122966930461a4490bc6b20f1
5/23/2018 14:10	18	66	7ab614a5aa280fd41d1be656cb7bff23f6e093e1f20869b6ae41c96c53de8550
5/23/2018 12:51	44	66	884c195efd779bfd1de130b3249d0249e8a868f6acacaf2aead9d0144599b051
5/22/2018 16:41	54	67	c59d16843567c776a16b4f8e8b28f751305eeb263a81310712c89dbd31d2fa55
5/21/2018 23:26	41	66	5142f62650a7411e6e45aac777b8028b50ed97c30f54bdbe8e607b088ebdc283
5/20/2018 14:17	44	67	5122e47006fdbd90396193e399e20bc790e95168577f2b07eac54289a43bfe72
5/18/2018 8:27	32	66	33161f7064aaafdc832fe297aec6b8be35df16c2a1bf69bfc21907fd227d9347
5/18/2018 8:12	28	66	4caa0b430bac83ca9cfcd6f891823c520dfadb25469dc9d300a7f8c5cdab84df
5/18/2018 3:32	47	62	c5acef7938d19ded69ba845ad917f5a0f4aaf5d4d63b777a1543e81fdf8f7aa1
5/17/2018 10:40	44	66	78ecd5b7e1d55680c8740d2de85913118d6f86380b25ee0d62a4837ee076d382
5/17/2018 10:32	42	66	fe09300643f9cbfb91c7dc56323afb53e159a2f5a9be2905e2ba2654c53ee660
5/17/2018 10:12	43	66	4703474b3ee29591b8c6983038f93938f5c5e99d6fd34d35c3d3d3d15c437a29
5/15/2018 9:01	36	65	a272bdb76a5b4e45d3010feb8463cc7a759bad14b85822dcc89b868a9dd37d98
5/15/2018 0:15	40	66	9b0cc8f94d30a364c0c1816f3021230134e323a1a185e5e96d12b65a703d0808
5/14/2018 7:52	42	66	7058bbece2e3c56f6106e9ee2a8978378dba6b8914cdd586bf87e5563840de25
5/12/2018 20:51	30	66	c161d8c8ecd7c285decc49ce7b2fee4c7cbe803976d25000cd084af7a85b3213
5/12/2018 17:43	16	66	cd2ba56f045b7493adca7af519d27ceea29ae253eae194f162c361da1145d6f4
5/12/2018 16:39	25	66	89cb35e00ab4460fa47ee7784fe9005953235513e2e0eb051038e1ad7158f078
5/12/2018 16:25	51	66	ed19464772c656df86dc1769584f2002010065172d6006a44c11977a1ca4f8d8
5/11/2018 22:39	4	66	470d616888273e5d90f001fb858b9a6fa1dabdc803b1f6aa7962f5968c1b2804
5/11/2018 13:42	41	63	f5b5d2e1b0025b6b1bdb1975c9d04323d3ad6452f4e82f66a1e7202ae2c37b16
5/11/2018 5:05	42	67	00dfe6ac99c10ceb62c79b77db36b333dd829f432df01ba17ed66d3e1197328a
5/11/2018 4:51	39	66	066270e71979385279eaf2445ec17a6bf58c5b43075faa1aead3714539c52ffd
5/11/2018 2:07	34	67	0fda280bb93ecdbc4e4311b12395ed52da42fd2dfe583ce4f772af01bd6f2d39

5/10/2018 16:24	17	67	10c4af9852ebec7b2ec637f40043f121140c257ffb0ddd347807a3fb0780c16e
5/8/2018 19:34	30	67	d6f70e3e19b35e516b512cda2c513466b27bbaf1097b00917d6ebb5197f8943b
5/7/2018 21:21	44	65	74f4004a36772b5dd6b38662e6651783b0ec7e160266f10416f25a2886d6a8c9
5/7/2018 17:13	30	67	e21245ab4168f3cde144acd1cbe657af4670125afa9ca39e25b94a59b9ebb137
5/5/2018 18:42	47	67	e5cedbc711582141be112567bb54e698b66d0f3c233c3839ec553b3be6956956
5/3/2018 2:52	36	67	070bcc231756e5d80c7925cb5f2e1718a75cb314b317c686bfef79a5fd532d5b
5/2/2018 9:56	3	64	95733ce61b6a9c604a935730bc1287ca6240c86f728d927eddb1eb84a65c2b87
5/1/2018 12:59	37	67	8bbbf252e53212b4970e5e046a4ec24765b67d9ee223f7b626e5b007130c2726
4/30/2018 19:05	36	67	37c35123aa4e108ccabfb14c7298bf2fff8aa9fbb0917c66ef3889db72f626b3
4/29/2018 2:24	38	67	e54eeff9bc718962e3dfd79b9c6783e5b6de3691104f379dd5f6ad4fbb2dbea0
4/28/2018 21:44	42	67	f38da99ae52024c3884c0eed1d1e3eeab10a1d3826f47dea56ddbaa3df543ba4
4/28/2018 16:53	42	67	a66aef112a9e1641b358c52f5aa2bc77da9e73dec5774c535a9c9ce356341a1d
4/27/2018 21:49	41	67	4d36d317bffb08bcfe0955ddb855557980c58594b9295795fe108922224e8574
4/27/2018 21:29	45	67	3512d832cecd9ee45e93776e6b4658dd6a2fc771c71f583b04f313881f404d0e
4/27/2018 20:40	43	67	24e33320a677a6efe02bea31e272c7c4c25734fdd005fef9db84a291e1ba15a0
4/27/2018 19:18	40	66	5c13fd3ae97a9bed32ae1139f5958f49dc0f6def91321e9361ab1039b091a710
4/27/2018 17:47	39	67	61da8c13f09e2fa1d02eb932d32f04c742e33776bf94211d6423ddbfab2d48c0
4/27/2018 5:22	40	68	fc17587824b564182b1067a690509c45fe5e2d8b1616170fcc116600b7745e7f
4/27/2018 3:18	40	67	c4f2d21422126d8b23334c59f42656c089820c3438983dd78f4a8dd4529302c0
4/26/2018 20:41	11	67	53c9ea0ef71358a3288229868fbafc8d108bc2ba6cd0ef06eacd2a0742841a31
4/26/2018 20:33	11	66	63b3909a8bf4874602f10754c7e5889af740c8e3265dbd78f3a660bb1dd8d2b4
4/26/2018 16:57	41	63	82616522d3fe20306fe24f6cd6da7ffd2d40d8d86766ecbe6019b740c000a033
4/26/2018 14:39	8	66	9a6268f5ddc7341a6d6442c43960d3198e5d95ca9d90792a725010a19ddaa6b0
4/26/2018 14:32	43	65	79cadaba88d35d2e25c764b34c8cf447271a1e4336c66830360fad89a05c5445
4/26/2018 7:43	41	67	a4b3c7abada7fcdfcf3ef4bf7af2cd5594ba5ed87291fb82849c271d0dcdcf37
4/26/2018 0:38	46	68	580206a291e901310e3de4e9ec8be3941264604ddd893d89f64f0430598e7825
4/25/2018 21:11	46	67	93341ae42ff6e5d79d80de0a15290980aff684c3685306f107267462ff48ea71
4/25/2018 17:22	43	66	23782b4719fe32f804ff6dc183a3ad637cbb1f69fb4181630a43de9ca9a1c7bf
4/25/2018 14:09	41	66	4d23202bbafa06758c19b74343f5bf87a57de00eb1670c82ad069221a9b4368a
4/25/2018 9:06	46	67	35c559a22975cc336ebd91e26d9c840bbf7859e88c8ca8d83e5f0be405eaebc6
4/24/2018 10:04	9	66	9523264282b58388121cc8e8c80e25bed180a164bf612953c4526777dd3917ee
4/23/2018 16:51	43	67	7383c6978d06868f2826d2c486366da1931b5d3e889fc2e57634de0ae2bd812d
4/23/2018 16:44	43	67	2bb01c38ff1d65b15343ca34c7fe9c3cc563c267b7c66b7e32d385f1a88667cb
4/23/2018 16:41	42	67	914f0c41c94d14e2541499f37512cc69f43dfa4ab277440a7436dd63fbd1a6f1
4/23/2018 16:28	43	67	1793fbc48d798c6300cff0d8411e139718675d55532b4e33315ff8b4b9b500d5
4/23/2018 16:18	44	68	b5a029d960df3cf30d44db26013f81e6b4b323929f3caffae67e8b0359551daf
4/23/2018 16:14	39	68	510c48ce5493af15de416efc0e276b72bf1713ad68f0323c8c78051218386bd3
4/23/2018 7:34	47	68	bc201da9bf85d8c833836e91bc7395801e8feee7badf6651cb9cf5259974e07c
4/23/2018 5:30	46	67	f9caf7c8d918aac496d78b5e03fbda9b6b06e0e913555554986339f68f40b5a8
4/22/2018 23:49	46	67	041a30bbafb012f323217392258cf29ec7d2297ddee42e4a602570b4908e8a90
4/22/2018 23:41	48	67	69feca7503f82c65c0b744edbeaad1239f534aecd89586cb4ce7910b122b9eae
4/22/2018 23:32	47	68	4555b94f5ed7811e83b3d44bd7ffe1419ed2769c7bd75ca0fb5ac2f53dbc0895
4/22/2018 23:32	46	67	b1b26720b3ebec36a4757f204ce89672d4c629c0bcb346af38a9dbb00c435ae4
4/22/2018 20:55	38	68	4085bb9af336275ac67dc79c60c2c80aee45f09f08fb4afbe7a7048078b0a721
4/22/2018 19:57	42	68	b49d2460b578f2d36aaddac69e39ba166f3a6c326dbaf1879c79e52966405877

[i] Adapted from https:// .paloaltonetworks.com/atoms/tiltedtemple/
[ii] https://malpedia.caad.fkie.fraunhofer.de/actor/emissary_panda
[iii] https://attack.mitre.org/groups/G0027/
[iv] https://nvd.nist.gov/vuln/detail/CVE-2021-40539
[v] Adapted from https://unit42.paloaltonetworks.com/sockdetour/
[vi] https://nvd.nist.gov/vuln/detail/CVE-2021-44077
[vii] https://nvd.nist.gov/vuln/detail/CVE-2021-28799
[viii] https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
[ix] Tools used to support this ongoing research include ZoneCruncher from Zetalytics, VirusTotal from Google, TruSTAR from Splunk and others.