Cyber Event Investigation

December 10, 2024

Will Kittredge

ISIN 409: Network Forensics & Analysis

Initial Event Investigation Steps

1. Replayed packets:
   - `sudo tcpreplay -i eth1 -M10 /opt/samples/markofu/*.pcap`
2. Started examining realtime events feed in SGUIL.
3. Noticed that 321 events occurred where a rule for detecting an encrypted Remote Access Trojan session was tripped.
4. Viewed event transcripts to see what happened.

Why investigate?

The event message and occurrence count are concerning, and the network traffic does not match anything "normal" that I've previously seen. "Gh0st" appears at the beginning of the payload, is noticeably legible compared to the data the follows, and also fits hacker stereotypes. Based on that, I think further investigation is reasonable.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	45	so-eth1-1	3.4	2024-12-10 23:43:51	192.168.56.52	80	10.0.3.15	1081	6	ET INFO EXE - Served Inline HTTP
RT	1	so-eth1-1	3.83	2024-12-10 23:43:51	192.168.146.131	4444	192.168.146.132	1036	6	ET INFO PE EXE Download over raw TCP
RT	321	so-eth1-1	3.84	2024-12-10 23:43:53	172.16.150.20	1097	58.64.132.141	80	6	ET TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server
RT	5	so-eth1-1	3.85	2024-12-10 23:43:53	172.16.150.20	1097	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
RT	5	so-eth1-1	3.86	2024-12-10 23:43:53	172.16.150.20	1097	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic
RT	6	so-eth1-1	3.87	2024-12-10 23:43:53	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.421	2024-12-10 23:43:56	10.42.42.253	36406	10.42.42.56	5911	6	ET SCAN Potential VNC Scan 5900-5920
RT	5	so-eth1-1	3.422	2024-12-10 23:43:56	10.42.42.253	40328	10.42.42.56	3306	6	ET SCAN Suspicious inbound to mySQL port 3306

Initial and potentially related events (selected in yellow).

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so-eth1-1	3.87	2024-12-10 23:43:53	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.88	2024-12-10 23:43:53	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.92	2024-12-10 23:43:53	58.64.132.141	80	172.16.150.20	1098	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.100	2024-12-10 23:43:53	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.299	2024-12-10 23:43:54	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive
RT	1	so-eth1-1	3.353	2024-12-10 23:43:54	58.64.132.141	80	172.16.150.20	1097	6	ET TROJAN [ANY.RUN] Win32/Gh0stRat Keep-Alive

Keep-alive/heartbeat – could indicate that a session is still open.

```
Sensor Name: so-eth1-1
Timestamp: 2024-12-10 23:43:53
Connection ID: .so-eth1-1_84
Src IP:                 172.16.150.20 (Unknown)
Dst IP:                 58.64.132.141 (Unknown)
Src Port:               1097
Dst Port:               80
OS Fingerprint: 172.16.150.20:1097 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint:   -> 58.64.132.141:80 (distance 1, link: ethernet/modem)

SRC: Gh0st.....x.Kc` `....@....\..L@:8..,39U! 19[.."....!
SRC: (+.`.V.....(Q!....`....
SRC: Q...2...&..w...?@CI.a..8C.Q!.)B...@9....f.a.....L.I.K.–..../.54.` ...1.o...
DST: Gh0st.....x.c.....
DST: Gh0st.....x.....).)
DST: Gh0st.....x.c.....
SRC: .
DST: .
SRC: .
DST: .
DST: Gh0st.....x.c.....
SRC: .
DST: .
SRC: .
DST: .
```

Unusual-looking traffic.

Snort/SIEM Rule

What is the rule doing?

In a nutshell:

- Alerts on TCP traffic (on any port) going from our network to an external network.
- Connection must have been established (a 3-way TCP handshake was completed) and the packet data must have included “Gh0st” in the first 5 bytes of the payload [1].

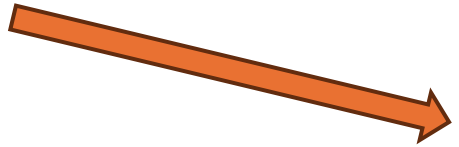
Potential improvement:

- We could try to remove the depth:5 condition, but this might match more traffic than we want. Updated versions of the malware might try to make traffic harder to identify by moving the “Gh0st” data, which seems to be some sort of anchor/identifier, to a different location.

```
Sensor Name: so-eth1-1
Timestamp: 2024-12-10 23:43:53
Connection ID: .so-eth1-1_84
Src IP:          172.16.150.20 (Unknown)
Dst IP:          58.64.132.141 (Unknown)
Src Port:        1097
Dst Port:        80
OS Fingerprint: 172.16.150.20:1097 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint:  -> 58.64.132.141:80 (distance 1, link: ethernet/modem)

SRC: Gh0st.....x.Kc`.`....@....\..L@:8..,39U! 19[.."....!
SRC: (+.`.V.....(Q!....`....
SRC: Q...2...&..w...?@CI.a..8C.Q!.)B...@9....f.a.....L.I.K.--..../.54.` ...1.o...
```

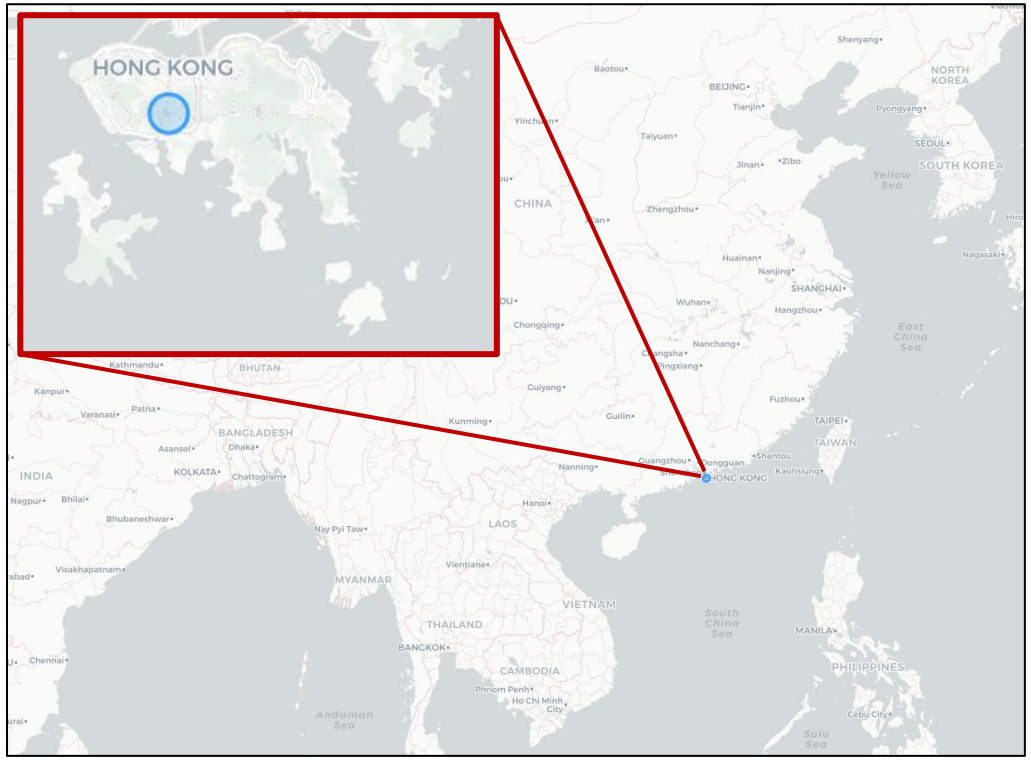
This traffic…



…triggered this rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Gh0st Remote Access Trojan Encrypted Session
To CnC Server"; flow:established,to_server; content:"Gh0st"; depth:5;
reference:url,www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network;
reference:url,www.symantec.com/connect/blogs/inside-back-door-attack; classtype:trojan-activity; sid:2013214;
rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2011_07_06, deployment Perimeter, malware_family Gh0st, malware_family PCRAT, signature_severity
Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2015_10_09;)
/nsm/server_data/securityonion/rules/so-eth1-1/downloaded.rules: Line 29569
```

GeoScope & Attribution



Map view (launched from Wireshark).

- The external address maps to a location in Hong Kong, China.
- According to a reference in the Snort rule, the gh0st remote access trojan was part of a Chinese cyber espionage operation – and one of its C2 servers was in Hong Kong [2, p. 32].

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 2 | UDP

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
58.64.132.141	211	12 k	105	6382	106	5940	Hong Kong	—	17444	HKBN Enterprise Solutions Limited
172.16.150.20	211	12 k	106	5940	105	6382	—	—	—	—

Wireshark IPv4 endpoint information (Alert ID 3.84).

Impact

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	so-eth1-1	3.85	2024-12-10 23:43:53	172.16.150.20	1097	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
RT	1	so-eth1-1	3.90	2024-12-10 23:43:53	172.16.150.20	1098	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
RT	1	so-eth1-1	3.102	2024-12-10 23:43:53	172.16.150.20	1099	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
RT	1	so-eth1-1	3.301	2024-12-10 23:43:54	172.16.150.20	1156	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102
RT	1	so-eth1-1	3.355	2024-12-10 23:43:54	172.16.150.20	1238	58.64.132.141	80	6	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102

Outbound traffic rules for the malware were tripped, but the traffic itself is not intelligible (see next slide).

I did not find any artifacts that can defend claims about how the gh0st RAT was initially downloaded or by whom. However, we know that the malware must have been executed based on the outbound traffic events recorded in SGUIL.

I have identified two possible explanations so far:

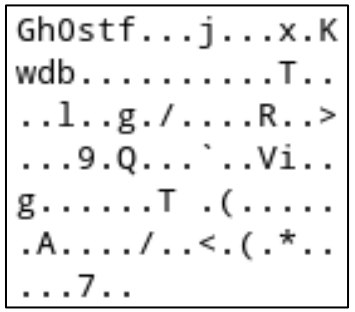
1. Information about the malware's download/origin was not captured.
2. The information was captured, but it hasn't been found yet.
   - Evidence suggests that the first sign of the malware is the from traffic that triggered the rule on slide 3.
   - I searched for other traffic involving the known Src IP, Dst IP, and for "Gh0st" at the beginning of packet payloads but did not uncover more information to suggest an origin.

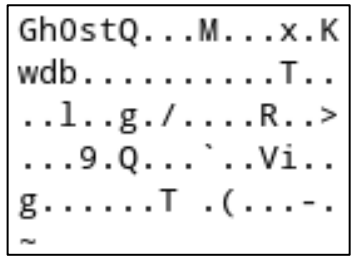
Concealment

In the gh0st RAT traffic that was detected, the only legible information is the first five bytes: “Gh0st”. The other payload data is unintelligible and presumably encrypted.

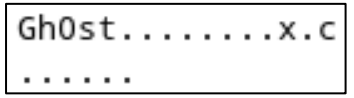
At least some useful information is exposed, though. Repeated identical payloads lead me to believe that the RAT has keep-alive/heartbeat functionality.

Apart from this, I did not locate artifacts that could suggest additional forms of concealment like erasing log files on the endpoint. However, this does not mean that more concealment methods aren’t being used.



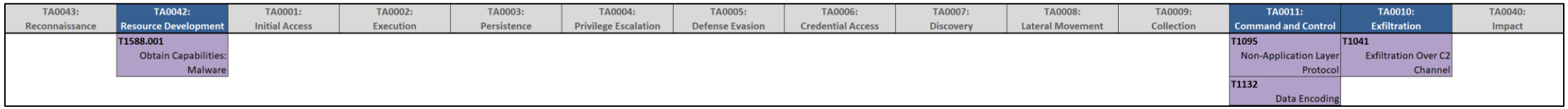


The traffic appears encrypted, and the relatively low amount of data suggests that this is command and control instructions rather than (for example) a mass exfiltration of secret or otherwise sensitive data.



Repeated payload.

MITRE ATT&CK Chart and Table



Tactics	Techniques	Threat Actor Artifacts/Activity	MITRE ATT&CK Reference URL
TA0001: Resource Development	T1588.001: Obtain Capabilities - Malware	The attacker obtained malware, in this case a remote access trojan, for use - its presence was detected on the network.	https://attack.mitre.org/techniques/T1588/001/
TA0011: Command and Control	T1095: Non-Application Layer Protocol	A non-application layer protocol was used in communications between the host and the suspected C2 server.	https://attack.mitre.org/techniques/T1095/
	T1132: Data Encoding	Data transmitted over the C2 channel was encoded.	https://attack.mitre.org/techniques/T1132/
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	Data was exfiltrated. In this case, we do not know exactly what was exfiltrated. There are no indications of a large file transfer to indicate a large amount of data theft, but that possibility cannot be ruled out.	https://attack.mitre.org/techniques/T1041/

The presence of the tactics and techniques listed above can be supported by the artifacts that I located.

I believe that, realistically, the gh0st malware is probably using more tactics/techniques than are listed here [3], but I did not find artifacts that can support this claim.

Conclusions & Recommendations

Potential chain of events:

1. gh0st RAT malware made its way to a host on the network and was executed.
    - Traffic/artifacts related to this might not have been captured.

2. The 172.16.150.20 host became infected and began communicating with the 58.64.132.141 host.
    - Evidence suggests that the external address (58.64.132.141) could be a C2 server located in China.

3. Events detecting outbound traffic and a keep-alive payload occurred.
    - This suggests that the malware exfiltrated some amount of data.
    - We are uncertain what the contents of the outbound data were because it appears encrypted.
    - Repeated observations of the keep-alive mean that the malware is probably still active.

Thoughts & recommendations:

1. We should assume that the initial access method still works.
    - I did not find evidence to suggest otherwise.
    - Secrets could have been exfiltrated, but small amounts of payload data make me believe that only basic C2 information has been exchanged so far.
    - References in the SIEM rule make me believe this was done for espionage purposes.
    - We know that outbound communications happened, but we don't know what the decrypted contents were.

2. Non-destructively investigate affected systems.
    - Because the traffic and detection rule suggest that the malware is for espionage and remote access, I believe we should take the event seriously.
    - Understanding the malware's capabilities will help us determine the event's severity and next steps (e.g., re-image devices, search for leaked secrets on the net, determine if a data breach occurred).
    - Consider isolating affected non-essential assets depending on investigation findings.
    - It may be wise to involve additional analysts at this point, as I could not find all the information we want.

References

[1] Cisco Talos Detection Response Team. (n.d.). *Payload detection rule options*. Snort 3 Rule Writing Guide. Retrieved December 10, 2024, from https://docs.snort.org/rules/options/payload/

[2] Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. (2009). Tracking GhostNet: investigating a cyber espionage network. In Tracking GhostNet: investigating a cyber espionage network. Munk Centre for International Studies, University of Toronto.

[3] *Gh0st RAT*. (n.d.). MITRE ATT&CK. Retrieved December 10, 2024, from https://attack.mitre.org/software/S0032/