02/12/2020 - Goblin Panda APT: Recent infrastructure and RAT analysis

meltx0r.github.io/tech/2020/02/12/goblin-panda-apt.html

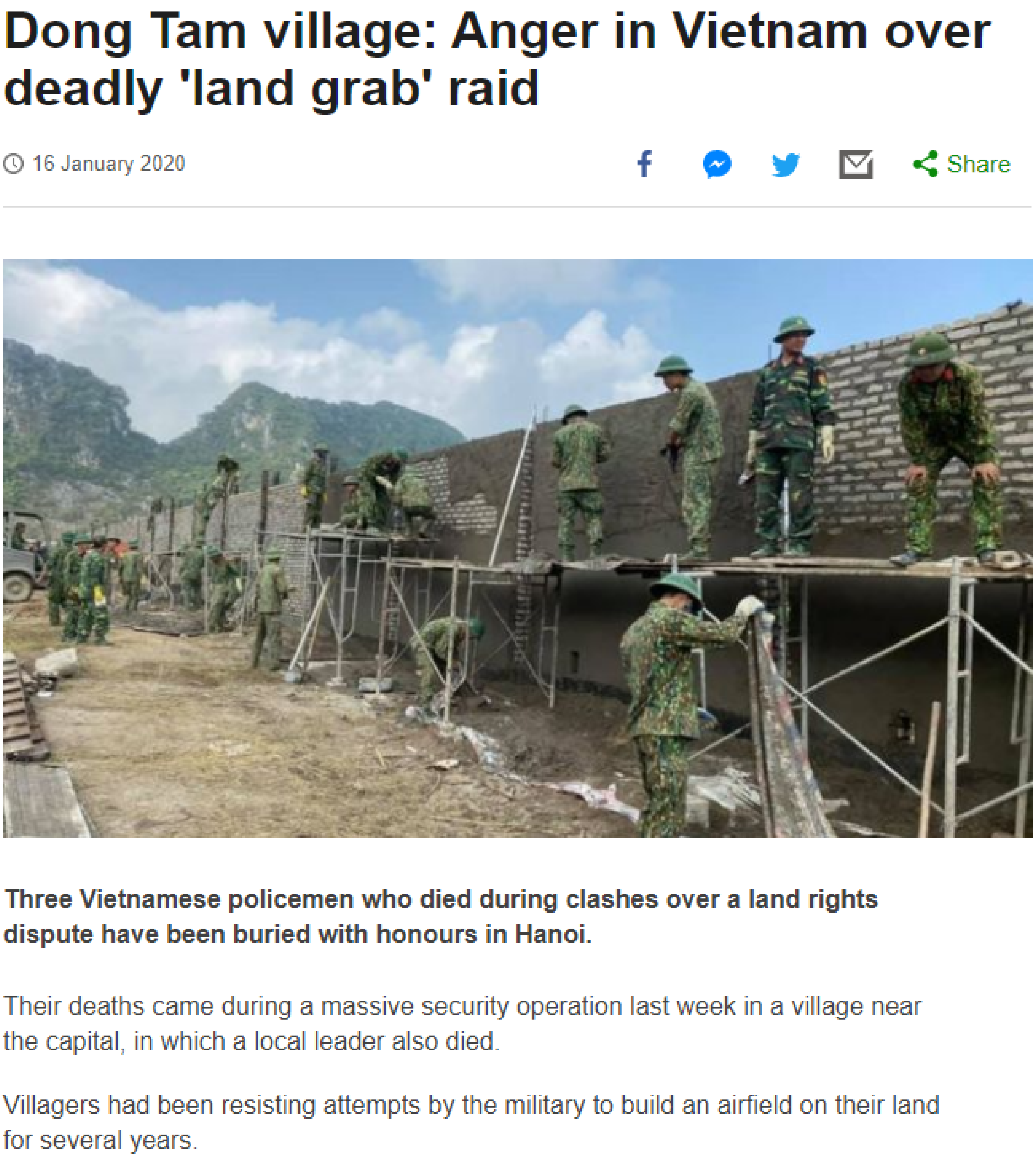
MELTX0R February 12, 2020

Summary

Goblin Panda (also known as Hellsing, Cycledek, and likely other names due to non-standardized naming conventions in security) is a group has been active for the better part of the last decade, and has historically had information theft and espionage related motives that align with Chinese interests. Their targets have primarily been defense, energy, and government organizations located in South/Southeast Asia, with emphasis on Vietnamese targeting. Within this analysis I review artifacts that exhibit behavior consistent with past Newcore RAT samples, which have been attributed to the GoblinPanda APT group.

Analysis

While reviewing suspected dropper files, I came across an interesting document titled *“Bao Cao Su Kien Dong Tam.doc”*, which translates to *“Report the Dong Tam event”* in Vietnamese. This document was created on 01-10-2020 at 08:31:00, and purported to contain information about a recent controversy regarding land disputes between the Vietnamese government and the locals of Dong Tam (a rural commune located in Hanoi, Vietnam). While this is not the first time tensions were high between Dong Tam locals and the Vietnamese government, the timing of the most recent events and the document creation date is quite suspect, with the most recent dispute occurring on 01-09-2020 - the day prior to the document creation.



Dong Tam village: Anger in Vietnam over deadly 'land grab' raid

16 January 2020

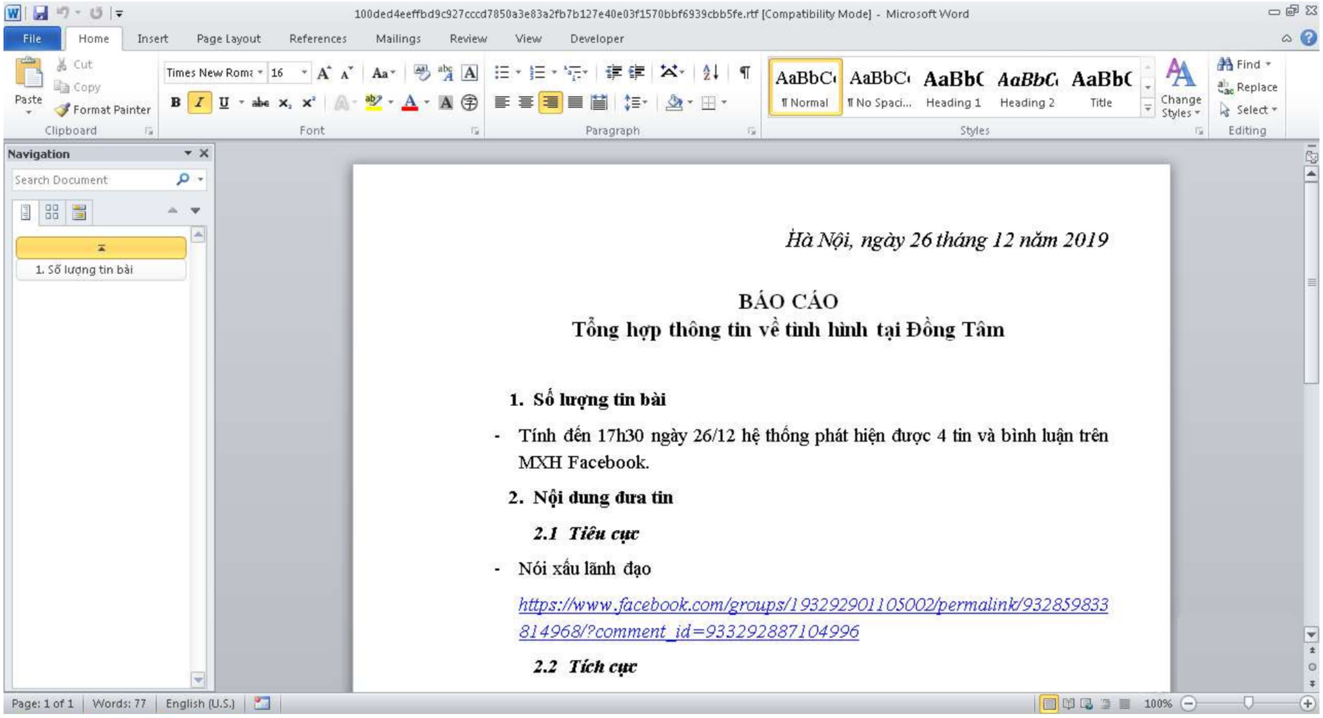
Three Vietnamese policemen who died during clashes over a land rights dispute have been buried with honours in Hanoi.

Their deaths came during a massive security operation last week in a village near the capital, in which a local leader also died.

Villagers had been resisting attempts by the military to build an airfield on their land for several years.

Shown above: Recent news headlines about Dong Tam village (source)

Upon opening the document, *CVE-2017-11882* is silently executed in the background. *CVE-2017-11882*, which was patched by Microsoft in November of 2017, is a memory corruption vulnerability which grants the attacker RCE (remote code execution) upon the user opening a specially crafted file (see here for the Microsoft advisory).


100ded4eeffbd9c927cccd7850a3e83a2fb7b127e40e03f1570bbf6939cbb5fe.rtf [Compatibility Mode] - Microsoft Word
Navigation
1. Số lượng tin bài
Page: 1 of 1
Words: 77
English (U.S.)
100%

Hà Nội, ngày 26 tháng 12 năm 2019

BÁO CÁO
Tổng hợp thông tin về tình hình tại Đồng Tâm

1. **Số lượng tin bài**

- Tính đến 17h30 ngày 26/12 hệ thống phát hiện được 4 tin và bình luận trên MXH Facebook.

2. **Nội dung đưa tin**

2.1 Tiêu cực

- Nói xấu lãnh đạo

https://www.facebook.com/groups/193292901105002/permalink/932859833814968/?comment_id=933292887104996

2.2 Tích cực

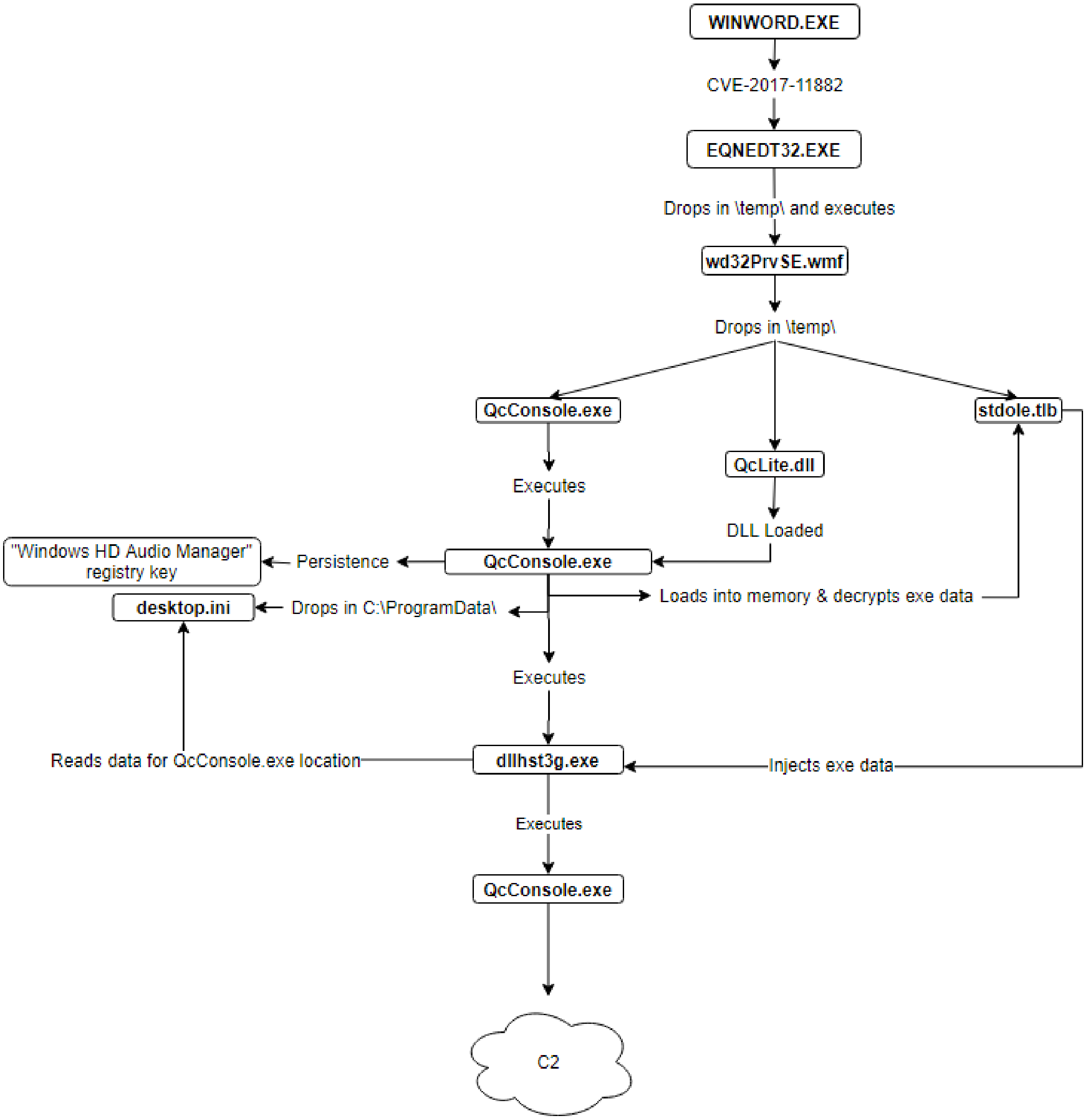
Shown above: Suspected Goblin Panda APT Lure “Bao Cao Su Kien Dong Tam.doc”

Following exploitation, an embedded object “wd32PrvSE.wmf” is dropped to the user’s local temp directory, and subsequently executed. Wd32PrvSE.wmf then drops three files to the user’s local temp directory - *QcConsole.exe*, *QcLite.dll*, and *stdole.tlb*. While *QcConsole.exe* appears to be a valid and signed file belonging to *McAfee, Inc.* the other two dropped files (*QcLite.dll* and *stdole.tlb*) have less than benevolent intentions.

It should be noted that, at the time of this writing, the document, wd32PrvSE.wmf, QcLite.dll, and stdole.tlb have very low or nonexistent detection rates of only 15/58 (document), 0/56 (WMF), 3/68 (DLL), and 0/56 (TLB) on VirusTotal, respectively.

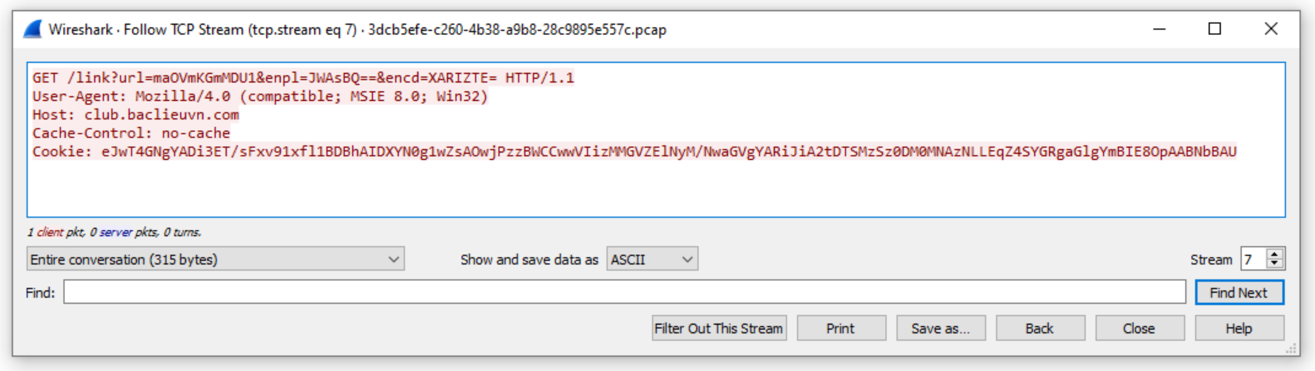
QcConsole.exe is then executed, and loads *QcLite.dll*. *QcLite.dll* will then establish persistence via an autorun registry key named *“Windows HD Audio Manager”*, drop a file titled *“desktop.ini”* to the *C:\ProgramData\* directory containing obfuscated data, and load the contents of *stdole.tlb* to memory, and decrypt it, resulting in executable data.

Dllhst3g.exe, a legitimate Windows binary, is then started in a suspended state, injected with the executable data extracted from *stdole.tlb*, and is subsequently resumed. The compromised *dllhst3g.exe* then decodes the contents of the previously dropped *“desktop.ini”* file, which directs it to the location of *QcConsol.exe*, and *QcConsol.exe* is executed for a second time.



Shown above: Execution graph

Command & Control communications are then initiated via the secondary *QcConsol.exe* process to the URLs *“hxxp://club[.]baclieuvn[.]com:8080/link?url=maOVmKGmMDU1&enpl=OXco&encd=XARIZTE=”* and *“hxxp://club[.]baclieuvn[.]com/link?url=maOVmKGmMDU1&enpl=OXco&encd=XARIZTE=”*. While this domain currently resolves to the Singapore IP Address *103.253.25[.]15*, none of the C2 requests received a response. This may be due to the infrastructure being burnt or specific geolocation requirements.


Wireshark · Follow TCP Stream (tcp.stream eq 7) · 3dcb5efe-c260-4b38-a9b8-28c9895e557c.pcap
1 client pkt, 0 server pkts, 0 turns.
Entire conversation (315 bytes)
Show and save data as
ASCII
Stream
7
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
GET /link?url=maOVmKGmMDU1&enpl=JWAsBQ==&encd=XARIZTE= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: club.baclieuvn.com
Cache-Control: no-cache
Cookie: eJwT4GNgYADi3ET/sFxv91xfl1BDBhAIDXYN0g1wZsAOwjPzzBWCCwwVIizMMGVZElNyM/NwaGVgYARiJiA2tDTSMzSz0DM0MNAzNLLEqZ4SYGRgaGlgYmBIE8OpAABNbBAU
```

Shown above: Packet capture of suspected Newcore RAT C2

Although I was unable to obtain additional C2 communications, the activity observed in relation to the dropped artifacts is very reminiscent of Newcore Remote Access Trojan. Furthermore, the targeted nature of the weaponized document, in addition to the apparent targeting of Vietnamese individuals, is quite suspect. While this isn't conclusive evidence that Goblin Panda is responsible for this sample, the similarities between it and other confirmed Newcore RAT samples, in addition to the fact that Vietnam has historically been targeted by Goblin Panda, is telling.

Indicators

Indicator	Type	Description
club.baclieuvn.com	Domain	Newcore RAT Command & Control server
103.253.25.15	IP Address	IP Address hosting Newcore RAT Command & Control server "baclieuvn.com"
/link?url=maOVmKGmMDU1&enpl=OXco&encd=XARIZTE=	URI	Newcore RAT Command & Control URI Pattern
/link?url=maOVmKGmMDU1&enpl=JWAsBQ==&encd=XARIZTE=	URI	Newcore RAT Command & Control URI Pattern

e9ba8cc1119dc4a972d0d363edcc0101	MD5	Bao cao su kien Dong Tam.doc - suspected Goblin Panda dropper
42c1a3a74cec2dc4a1c1a7a10d9d14e4	MD5	QcLite.dll
6d1876c07d176185dc61310b9aa510fe	MD5	stdole.tlb
7edeb624f2fef843ed26f24f3dd01a3f	MD5	wd32PrvSE.wmf

References/Further Reading

1. https://www.fortinet.com/blog/threat-research/cta-security-playbook–goblin-panda.html
2. https://medium.com/@Sebdraven/goblin-panda-continues-to-target-vietnam-bc2f0f56dcd6
3. https://app.any.run/tasks/b64134d1-b809-4ff8-bcb0-91c18425c541/
4. https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf
5. https://unit42.paloaltonetworks.com/unit42-analysis-of-cve-2017-11882-exploit-in-the-wild/
6. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/
7. https://www.bbc.com/news/world-asia-51105808