CS7038 - Malware Analysis - Wk07.2

Malware Research Online

Coleman Kane
kaneca@mail.uc.edu

February 22, 2018

Exploring the Online Ecosystem

One nice aspect of malware analysis is that, since much of it originates online and primarily impacts users that rely upon the Internet, many of the communities doing malware research have established online presences.

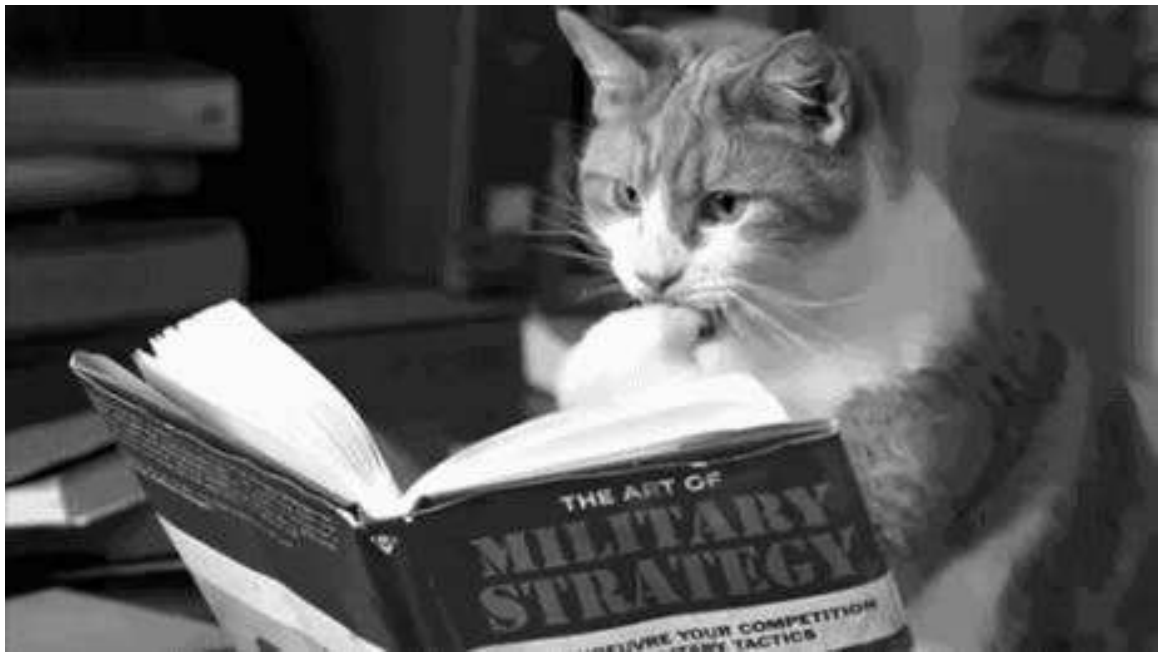
We will discuss various resources that exist online, and also take some time to dive deeper into what they have to offer.

In some cases, you can get narratives describing attacks, while in other cases you can get documentation and reports discussing specific families of malware. Sometimes you can actually retrieve real malware artifacts as well.

Attack Descriptions Online

A great resource, though not so user friendly, is the "APTnotes" repository hosted on GitHub. The content of the repository is a structured index of a large number of cyber intelligence reports going back to $\tilde{2}008$. They've been archived in the author's *box.com* account.
`https://github.com/aptnotes/`

The **ThreatMiner** project offers a really nice searchable UI for this dataset:
`https://threatminer.org`



UNIVERSITY OF Cincinnati

OilRig Spearphish

An attack that has been observed targeting Israel and other middle eastern countries. A report was published by ClearSkySec (`http://www.clearskysec.com`) earlier in 2017.
`https://github.com/aptnotes/data/issues/83`

The adversary allegedly compromised the network of multiple IT services vendors, and used this access to send *spearphishing* emails to their targets. These emails contained a URL, similar to below, as well as a username and password. The message informed the recipient that the sender wanted their feedback in testing the system. It expressed urgency in the recipient getting back to the sender with feedback.
`https://_____/dana-na/auth/url_default/welcome.cgi`

Look familiar?
`https://sslvpn.uc.edu/dana-na/auth/url_default/welcome.cgi`

In fact, they did an exemplary job of making a system that mimics a Juniper VPN login.

OilRig Fake VPN

The adversary not only copied the HTML for the website, but also hosted a fake VPN client on it.

In a traditional Web-based VPN software setup:

1. You will visit the webpage for your organization's VPN
2. You use your credentials to log into the VPN
3. The Web-based application will perform some checks to determine if you have a VPN client installed
4. If not, you will be presented with the option to install one, by downloading and executing an installation program - typically expected to involve providing administrative rights to the installer

In this example, rather than a legitimate Juniper VPN installer, the adversary offered a fake one that installs a backdoor on the system, instead of a VPN connection client.

To the user, the behavior presents as expected.

Operation Double Tap, Suspect FireEye APT3

In this attack in 2014, a well known threat group known as **APT3** to FireEye, is alleged to have sent a large amount of phishing attacks. Contrary to historic attacks from this adversary, this event was themed using a NSFW "spam-like" theme to deliver a backdoor.
Earlier in 2014, the adversary has been alleged to have delivered malware via Facebook direct messaging.

`https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html`

`https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html`

This attack was novel for a number of reasons:

- Departure from historic themes that attempted to appear work-related
- Attacks using social-media, non-email vector
- New malware (*MyRat* and *MShell*)

Operation Double Tap Attack

In the *Operation Double Tap* attack, multiple malware layers were employed to achieve the objectives.

1. Spearphish email sent containing a link to sign up for entertainment service
2. Webpage at sign-in contains two malware vectors built in (*Trojan*):
   (a) VBscript built into the webpage to invoke an EXE downloaded from the website (`install.exe`)
   (b) An IE exploit that would work in versions of Windows prior to supporting powershell and would download and run `install.exe`
3. The `install.exe` writes two files to disk (`doc.exe` and `test.exe`) (*Dropper*)
4. `install.exe` executes `doc.exe` which attempts to *escalate privilege* and then runs `test.exe`

Operation Double Tap Attack (cont.)

The `test.exe` program is a copy of the "MyRat" tool. Following the `doc.exe` execution, the `test.exe` program next attempts the following:

- Checks current user permission
- Creates a "scheduled task", like a UNIX cron job, to execute `test.exe` on log in
- Constructs a command-and-control channel with a remote server

Upon behavioral analysis, its determined to be a *backdoor*.
Further analysis, documented in the report, demonstrates that it has the following hard-coded behavior:

- Reads, Writes, Executes the files `notepad.exe`, `notepad1.exe`, `newnotepad.exe`, `notepad2.exe`, `note.txt` in a Windows Temporary files folder

Operation Double Tap Classification

Based upon the above discussion, we can apply the classification methods from last lecture to this attack:

Familial
The malware samples were identified as projects named "MyRat" and "MShell". It appears likely that both of these were written by the same author or team of authors.

Functional
The attack utilizes some *Trojan* components, such as the initial website, as well as the `install.exe` delivered to the user. There is a *backdoor* `test.exe`. And there is also a *dropper* function in `install.exe`

Behavioral
The `install.exe` exhibits the *behavior* of writing files named `doc.exe` **AND** `test.exe` to disk. The file `doc.exe` exhibits the behavior of leveraging the CVE-2014-4113 exploit to escalate privileges. The `test.exe` program exhibits the behaviors of reading, writing, and executing files within a Windows temporary folder.

US Federal Indictments

In late 2017, Chinese nationals alleged to be connected to the APT3 operation were indicted. Though this wasn't delineated in the indictment, a number of security professionals who had been tracking this group connected the dots.

Indictment:

https://www.justice.gov/opa/pr/

us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

Research:

https://intrusiontruth.wordpress.com/2017/04/26/

who-is-behind-this-chinese-espionage-group-stealing-our-intellectual-property/

https://intrusiontruth.wordpress.com/2017/05/02/who-is-mr-wu/

https://intrusiontruth.wordpress.com/2017/05/05/who-is-mr-dong/

https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/

http://freebeacon.com/national-security/

pentagon-links-chinese-cyber-security-firm-beijing-spy-service/