Legal Informatics, Privacy and Cyber Crime

Part Two: Attack Theory

Sandro Etalle

02/05/2018

2017/2018
About this part of the course

• Topic: how cybercriminals usually structure their attacks

• Underlying material: book,
  – Ch 1, 2, 3
  – Ch 4: only 4.1, 4.2, 4.5
Chapter 1, some points

Today, the majority of nation states are developing cyber war capabilities. **Zero-day exploits in critical software** ... are now considered to be attack weapons.

Question: what are zero-day exploits and why are they considered weapons?

**There exists several definitions of targeted cyber attacks.** We adhere to a basic definition based on the naming convention—a targeted attack is a class of dedicated attacks that aim at a specific user, company, or organization to gain access to the critical data in a stealthy manner. **Targeted attacks should not be confused with broad-based attacks** that are random in nature and focus on infecting and compromising large groups of users.

The boundary between targeted attack and broad-based attacks is getting weaker. There are campaigns (e.g. Havex, Epic Turla), that have the features of targeted attacks (customization, stealth, etc), but they actually target a number of companies (in the case of Havex, Energy companies).
Features of Targeted Attacks

According to the book:

Some important characteristics of targeted attacks are as follows:

- Zero-day exploits against unknown vulnerabilities are used to compromise target systems so that the attacks are not easily detectable.
- Sophisticated malware families (custom coded) are used, which go unnoticed despite the presence of security solutions installed on the network and end-user systems.
- Real identity behind the attack is hidden to keep a low profile to avoid any legal problems.
- Systems having no value in the attack campaign are not infected and compromised. This in turn lowers the exposure of the attack and makes it stealthier.
- Attack is made persistent for a long period of time and operations are executed in a hidden manner.

TRUE in many cases but not all of them
Targeted attacks vs APTs

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Targeted Cyber Attacks</th>
<th>APTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deceptive</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Stealthy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Exploits</td>
<td>Both known/unknown exploits</td>
<td>Primarily, zero-day exploits are used</td>
</tr>
<tr>
<td>Persistent</td>
<td>Depends on the design</td>
<td>Yes</td>
</tr>
<tr>
<td>Data exfiltration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintaining access</td>
<td>Yes: Remote Access Toolkits (RATs)</td>
<td>Yes: RATs</td>
</tr>
<tr>
<td>Intelligence reuse</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lateral movement</td>
<td>Depends on the design</td>
<td>Yes</td>
</tr>
<tr>
<td>Campaigns</td>
<td>Depends on the design</td>
<td>APTs are started as campaigns</td>
</tr>
<tr>
<td>State sponsored</td>
<td>Possible</td>
<td>Possible</td>
</tr>
<tr>
<td>Actors</td>
<td>Individual or group</td>
<td>Group</td>
</tr>
</tbody>
</table>

- Do not agree completely with the table
- What does it teach us?
Some known (and by now old) targeted attacks

<table>
<thead>
<tr>
<th>Targeted Attacks (or APTs)</th>
<th>Month/Year Started (Approx.)</th>
<th>Known/Zero-Day Vulnerability/Exploit</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>GhostNet (Gh0st Net)</td>
<td>March 2009</td>
<td>Known/zero-day</td>
<td>Dalai Lama’s Tibetan exile centers in India, London, and New York City, ministries of foreign affairs</td>
</tr>
<tr>
<td>Aurora (Hydraq)</td>
<td>January 2010</td>
<td>Yes, Internet Explorer and Perforce software were exploited</td>
<td>Approx. 34 US companies such as Google, Juniper, Rackspace, etc.</td>
</tr>
<tr>
<td>Stuxnet</td>
<td>June 2010</td>
<td>Four zero-day exploits including Shortlink (CPLINK) flaw were used including known vulnerability</td>
<td>Iran nuclear facilities using Siemens infrastructure</td>
</tr>
<tr>
<td>RSA breach</td>
<td>August 2011</td>
<td>Yes, Adobe flash player</td>
<td>RSA and defense contractors using RSA security solutions</td>
</tr>
<tr>
<td>Duqu</td>
<td>September 2011</td>
<td>Yes, MS Word True Type (TT) font vulnerability was used</td>
<td>Worldwide ICSs</td>
</tr>
<tr>
<td>Nitro attack</td>
<td>July 2011</td>
<td>Malicious files are extracted from the attachment. Known and unknown exploits were also used</td>
<td>Approx. 29 chemical companies</td>
</tr>
<tr>
<td>Taidoor attack</td>
<td>October 2011</td>
<td>Approx. nine known vulnerabilities were used</td>
<td>US/Taiwanese policy influencers</td>
</tr>
<tr>
<td>Flame (SkyWiper)</td>
<td>May 2012</td>
<td>Yes, Terminal Service (TS) licensing component was exploited to generate rogue certificates</td>
<td>Cyber espionage in Middle East companies</td>
</tr>
</tbody>
</table>
The steps in a targeted attack

For this I prefer to use Lockheed Martin cyber kill chain

- **Reconnaissance**
- **Weaponization** preparation of the attack, gathering of tools
- **Delivery** e.g. via phishing of watering hole
- **Exploitation** the first infection
- **Installation** of the full malware
- **Command and Control** connects home to update itself and receive commands. Possible lateral movement. Some data exfiltration starts taking place.
- **Action on Objectives** could be data exfiltration, or something else

Network Level Security

• There is a nice table (2.1) with a list of tools that can be used for intelligence gathering.

• There are many tools for OSINT (Open Source Intelligence Gathering).

• For instance: Maltego, creep.py, The Harverster, ..); if there is time we (you) can install them to see how easy it is to trace someone and let him “go” where you want him to be
Other Interesting tools to experiment with

- Interesting experiment to do: install FOCA
- [https://www.elevenpaths.com/labstools/foca/index.html](https://www.elevenpaths.com/labstools/foca/index.html), and play with it

- “FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans. These documents may be on web pages, and can be downloaded and analyzed with FOCA.

- It is capable of analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files, although it also analyzes Adobe InDesign or SVG files, for instance.

- These documents are searched for using three possible search engines: Google, Bing, and DuckDuckGo. The sum of the results from the three engines amounts to a lot of documents. It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.”
A spear phishing attack was used against the RSA Corporation which is named as “RSA Secure ID Breach.” The overall damage of this attack is not determined, but it is assumed that attackers stole Secure ID product information and number of token seeds used by several companies (organizations) such as Bank of America, Lockheed, JPMorgan Chase, Wells Fargo, and Citigroup. In **RSA Attack**, the attacker targeted two different batches of employees over a period of 2 days with a well-crafted phishing e-mail. The e-mail carried an XLS file containing exploit code of a then unknown vulnerability. Figure 3.2 shows how the phishing e-mail targeting **RSA looked like**. There could be other variants, but this one was widely distributed.
The RSA hack (part 2)

The attachment carried an exploit code of a zero-day for Adobe Flash Player vulnerability which was later identified as CVE-2011-0609. Once the exploit was successfully executed, the malware took control of internal servers. The attacker then used a RAT named as Poison Ivy [3] to take persistent control over the target servers. The stolen information was compressed and exfiltrated from the infected system using the FTP.

Questions: explain CVE-2011-0609, RAT, FTP, and how the could possibly have taken control of the internal servers.
### Table 3.1: An Overview of Structure of E-mails Used in Targeted Attacks in Last Years

<table>
<thead>
<tr>
<th>Targeted E-Mail Theme</th>
<th>Date</th>
<th>Subject</th>
<th>Filename</th>
<th>CYE</th>
</tr>
</thead>
</table>
| Job | Socio – Political ground               | 07/25/2012         | • Application  
• Japanese manufacturing  
• A Japanese document  
• Human rights activists in China | • New Microsoft excel table.xls (password: 8861)  
• qRJ(24.7.1).xls  
• 240727.xls  
• 8D823C0A3DAD8334B6C1974E2D6604F.xls  
• Seminar.xls | 2012-0158   |
| Socio - Political ground               | 03/12/2012 – 06/12/2012 | • TWA’s speech in the meeting of United States Commission for human rights  
• German chancellor again comments on Lhasa protects  
• Tibetan environmental situations for the past 10 years  
• Public Talk by the Dalai Lama_Conference du Dalai Lama Ottawa, Saturday, 28th April 2012  
• An Urgent Appeal Co-signed by Three Tibetans  
• Open Letter To President Hu | • The Speech.doc  
• German Chancellor Again Comments on Lhasa Protects.doc  
• Tibetan environmental statistics.xls  
• Public Talk by the Dalai Lama.doc  
• Appeal to Tibetans To Cease Self-Immolation.doc  
• Letter.doc | 2010-0333   |
| Socio - Political ground               | 01/06/2011         | Three big risks to China’s economy in 2011                          | Three big risks to China’s economy in 2011.doc                                                                                              | 2010-3333   |
| Socio - Political ground               | 01/24/2011         | Variety Liao taking – taking political atlas Liao                     | AT363777.7z | 44.doc                                                                                                                       | 2010-3970   |
| Economic situation                     | 03/02/2012         | Iran’s oil and nuclear situation                                      | Iran’s oil and nuclear situation.xls                                                                                                         | 2012-0754   |
| Nuclear operations                     | 03/17/2011         | Japan nuclear radiation leakage and vulnerability analysis           | Nuclear Radiation Exposure and Vulnerability Matrix.xls                                                                                     | 2011-0609   |
| Nuclear weapon program                 | 04/12/2011         | Japan’s nuclear reactor secret: not for energy but nuclear weapons   | Japan Nuclear Weapons Program.doc                                                                                                             | 2011-0611   |
| Organization meeting details           | 06/20/2010         | Meeting agenda                                                         | Agenda.pdf                                                                                                                                    | 2010-1297   |
| Nuclear security summit and research posture | 04/01/2010     | Research paper on nuclear posture review 2010 and upcoming Nuclear security summit | Research paper on nuclear posture review 2010.pdf                                                                                           | 2010-0188   |
7: Why Targeted Attacks are so easy to carry out

• You can probably drive a car, but you cannot build one, right?

• Carrying out a cyberattacks is like driving a car

• Until a few years ago, you needed to craft your own attack (equivalent to building your own car” if you wanted to drive around)

• Today, you can buy the car, and drive it. (Actually, you can put together the car you want, it is a bit like the IKEA market for cyberattacks: you need to do some work to put it together, but anyone can do that).

• Let’s see how
This network cannot exist in practice, it just serves for illustration purposes.
Step 1a, get a host for your command and control

Just rent it on the black market. Our you can set up your own, but then you are more traceable

This network cannot exist in practice, it just serves for illustration purposes
Step 1b, put the right (C&C) software on it

You have to buy this on the black market. It is plenty of them on the internet. You haven’t written a line of code yet.

This network cannot exist in practice, it just serves for illustration purposes.
Step 2, gather intelligence about the target

Facebook, google ... use one of many specialized tools or ... ask the underground market.

- Which sites does he look at (important for watering hold)
- Which systems does he use? (important to select the exploits)
- What are his role and colleagues inside the organization? (for Spear Phishing)

This network cannot exist in practice, it just serves for illustration purposes.
Step 3: Choose the right exploit, to get “the foot in the door”

For instance, you know that the target uses Adobe Acrobat and you may choose an exploit that uses a vulnerability of Adobe.

This network cannot exist in practice, it just serves for illustration purposes.
Step 4: Choose the right malware

The Exploit is a small chunk of code that allows to get "in" the target.

The Malware is a much more complex framework that allows to "do" things after you have compromised the computer. Choose one depending on needs: keylogging, RAT? Spyware? Data exfiltration? Lateral Movement? Do you need privilege escalation?

This network cannot exist in practice; it just serves for illustration purposes.
Example: ProRAT toolkit
Step 4: Attack the target

Usually using
Watering holes or
Spear Phishing

Direct attacks are
less popular

This network cannot exist in practice, it just serves for illustration purposes
Step 4: Use it!

Now you usually have control on the end-system.

It can also wait for more commands from you to diversify the attack.

TBD: droppers, and Payload,

This network cannot exist in practice, it just serves for illustration purposes.
Step 4: perhaps you can steal the VPN credentials

And then connect directly to the VPN port of the switch, rather than via the CC.

QUESTIONS: WHAT ARE THE ADVANTAGES AND THE DISADVANTAGES OF THIS APPROACH?

This network cannot exist in practice, it just serves for illustration purposes.
Example of Lateral Movement (1)

Once inside, lateral movement is relatively easy, because “inside” there is usually very little authentication, and it is easy to steal credentials (e.g. via keylogging).

QUESTION: why can’t you attack the TV directly?

This network cannot exist in practice, it just serves for illustration purposes.
And then the TV/SCADA may be controlled by you either
- Via the previously compromised system
- Via the CC (the TV/SCADA can connect to the CC)
- Via … (there always other ways)

**QUESTION:** why can’t you attack the TV directly?

This network cannot exist in practice, it just serves for illustration purposes
Lateral Movement can get physical

Then you can also damage physical systems, e.g. the air conditioning (see StuxNet, Ukraine attacks, Triton/Triconex)

This network cannot exist in practice, it just serves for illustration purposes
Drive-by Download

1. Attacker exploits an existing, legitimate website

2. User browses to the compromised site

3. Hidden java exploit downloads malicious payload and executes it silently

4. Remote Access Trojan installed, opens reverse shell back to attacker

5. Attacker gains remote control
   - Privilege Escalation
   - Password gathering
   - Etc.

6. Attacker uses gathered passwords to move laterally and stage data on externally accessible company website.

7. Attacker retrieves staged data from victim company’s website
Browser Redirect and Malware Delivery
Other attack techniques

Watering holes

**USB attack:** not very common, but it was the method Stuxnet used to penetrate the system

**Direct attack:** anything hosting a service can be attacked if the software implementing the service has vulnerabilities

- **A webserver.** Examples: SQL injection, Cross-Site Scripting (XSS), …
- **A router at home.** Usually has some “ports” open for e.g. maintenance
- **CCTVs, Televisions, Fridges, Printers …** they all have a webserver, (discussion on isolation of networks, and firewalls)

“One notorious targeted attack was launched against Bit9 [13,14]. **Attackers exploited the Internet facing web server of Bit9 and conducted a successful SQL injection that provided access to the critical systems of Bit9.** SQL injection is an attack technique in which unauthorized SQL statements are injected as input values to different parameters in the web applications to manipulate the backend database.”
Example of a Direct Attack 1: the webserver (or the NAS you have at home that is reachable from outside)

Because the switch forwards some ports to the webserver, you can reach it. If you have an exploit for the webserver, you can install your RAT on it, or use it as a stepping stone.

Same reasoning applies to everything you have that is reachable from the outside (do you have a NAS? Also some thermostats...)

This network cannot exist in practice, it just serves for illustration purposes.
Example of a Direct Attack 2: the router

The router is usually reachable.

Disadvantage: may not be able to carry a full RAT, and you are not yet where the important information is.

But is is a very good stepping stone. E.g. to attacks systems that are never monitored: the TV, the printer….

This network cannot exist in practice, it just serves for illustration purposes.
QUESTIONS?