DATA AND NETWORK SECURITY

Case Study II: Duqu II

1

Overview

- Classification: Virus
  - Infects system to perform unauthorized operations
  - Advanced Persistent Threat
  - Level of sophistication: Nation/State
  - Timeframe: 2014-2015
- Targets:
  - P5+1 events & negotiations with Iran on a nuclear deal
  - Kaspersky Labs
  - Anti-virus vendor
- Purpose:
  - Cyber Espionage: Spy on Kaspresky research and development
  - No other disruption of systems noticed
- Etymology

2

Overview

- Effort: Experts estimate the level of sophistication:
  - Team of 5-30 talented developers
  - 6 months or more development time

3

4

Etymology (related viruses)

- Duqu II
  - appears to be variant of Duqu [2011]
- Duqu
  - apparently from same group as Stuxnet [2010]
  - Thought to have about 7 variants
- Duqu/Duqu II purpose was cyber espionage
  - Targeted infiltration of systems to extract data
- Stuxnet
  - purpose was industrial sabotage
    - Target PLC/SCADA devices (programmable logic controllers used to control other equipment)
    - Specifically infiltrated Iran nuclear refinement site and damaged several centrifuges.

Data Security: Case Study II : Duqu II [Tony Mione, SUNY Korea, 2020]

4

5

Major Attack Strategies

- Uses numerous zero-day vulnerabilities
- Entrance via infected MS Word file
  - Crafted True Type Font containing malware
  - Rare/sophisticated technique
- Two major phases
  - Network topology discovery
  - Lateral movement
- Contains various payloads
  - Each has a task/goal
  - Difficult to detect 'signatures'
    - Each is compressed with one of several compression algorithms
    - Each is encrypted with one of several encryption algorithms

Data Security: Case Study II : Duqu II [Tony Mione, SUNY Korea, 2020]

5

6

Detailed Infection Process

- Initial infection: Word document with malicious embedded TTF (True Type Font File)
  - Elevates to kernel mode
  - zero-day exploit (4CVE-2014-4148)
- Lateral movement
  - zero-day, (CVE-2014-6324)
  - Allowed unprivileged windows domain user to elevate privileges to 'domain administrator'
  - Now, create and deploy MS installer packages (MSI) to other machines
  - Start service to execute the MSIs on target machines

Data Security: Case Study II : Duqu II [Tony Mione, SUNY Korea, 2020]

6

7

Detailed Infection Process

- Lateral movement (cont)
  - MSI files contain malicious 'stub' code
  - The stubs load other malware resources and decrypt them then transfer control
  - Resources execute in 'layers'
    - ActionData (msi.dll)
    - ActionData0
    - Klif.dll – This tries to mimic Kaspersky modules
      - Code iterates through running processes looking for process with a hash of lowercase process name that is 0x3E3021CB,

7

8

Detailed Infection Process

- Resources execute in 'layers' [cont]
  - Attack AVP.EXE
    - Searches for path to avp.exe by searching product registry entries for following products:

KES12	AVP15	AVP10	AVP8
KES11	AVP14.0.0	KES9	AVP7
KES10	AVP14	KES8	AVP6
AVP16.0.0	AVP13	AVP80	
AVP16	AVP12	AVP90	
AVP15.0.0	AVP11	AVP9	

    - Confirms avp.exe location once path found
    - Does availability and access checks
    - Patches avp in memory
    - Through a series of thread creations and calls, tricks Kaspersky code into thinking certain calls are safe and trusted.

8

9

Detailed Infection Process

- Payloads – Malware modules contain a number of payloads for different 32 and 64 bit architectures
  - l – searches for and disables security packages (anti-virus, etc) from a number of vendors
  - g – Like module l but skips trying to hijack a 'security token'
  - q, l, k – These are similar but vary:
    - Thread in which they run
    - How they inject code into security executable
    - Whether new thread blocks current thread or not

9

10

Platform Plugins

- Basic backdoor module distributes packages to other machines on the lan
- Packages include plugins with numerous functions
  - **Duqu 2 orchestrator** – Communication with C&C
  - **Basic System Information**
  - **Windows Socket based transport**
  - **Exfiltration module** – Sends files out
  - **File and Directory Manipulation**
  - **Network/Domain Dis**covery – Enumerates servers, users, network shares
  - **Network Infection module** – Tries to acquire administrative credentials from running processes
  - **Collect System Information** – USB attaches, drive history
  - **Extensive system & user info collection**

10

11

Platform Plugins

- Packages include plugins with numerous functions (cont)
  - **Utility DLL** – For creating new MSI packages
  - **MYSQL Discovery** – locate mysql servers
  - **File System Discovery** – Enumerate file shares
  - **Password Stealers** – Google Chrome and Firefox credentials, LSASS, SAM cache, POP3, HTTP, IMAP passwords, etc.
  - **Additional modules to collect system and network information**
  - **Sniffer based network attack modules (3+)**
  - **File system survey and utilities**

11

12

Persistence Mechanism

- Duqu remains mostly in memory (not disk)
  - Avoid detection by Anti-APT technology
  - Makes it difficult to do forensic analysis
  - Requires extra, alternate persistence mechanism to survive reboots
- Picks high-availability servers to infect
  - These servers monitor and reinfect machines within LAN when rebooted
  - Massive power failure may disinfect a site
  - However, site can be reinfected using stolen credentials

12

13

C & C (Command and Control)

- Deploys several C&C intermediate servers on LAN
  - These relay messages to C&C server outside LAN
  - Usually planted on high-uptime servers
- C&C communication hidden
  - Network pipes
  - Masking traffic inside image files

13

14

Sources

- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf
- https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/
- https://securelist.com/duqu-faq-33/32463/
- https://en.wikipedia.org/wiki/Stuxnet

14