LIFARS
your digital world, secured

Case Study – Phishing test

LIFARS regularly conducts phishing tests, in addition to penetration tests to ensure implemented security measures remain effective, maintain strong, and can upload to real world scenarios. Although, advancing technologies can strength security protection of organization, the human factor remains. Human behavior is often targeted and exploited by attackers using techniques like social engineering to send out carefully crafted phishing emails.

LIFARS cyber resiliency experts can simulate threat actors and their tools, tactics and procedures (TTP) to prepare and deliver advanced phishing attacks for our clients in safe manner. Upon client request, our experts can also simulate APT attacks, including creating customized malware samples made to bypass security detections.

" If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier

During a Red Teaming engagement our client requested LIFARS to conduct a black box phishing test. As a Fortune 500 company, the client has strong protection technologies in place and regularly verifies the effectiveness of the technologies through penetration tests. The client is aware of the risks its employees face from phishing emails sent by real attackers, and therefore, requested we perform an advanced phishing test. This test is prepped with the purpose of delivery and execution of "malicious" code provided by "attacker" in their infrastructure. In other words, they requested LIFARS to develop a customized malware capable of remaining undetected by their security solutions but can also deliver proof of its execution.

During this assessment LIFARS experts had to gather intelligence info, such as email addresses of potential victims, develop custom malware and bypass the various protections of the up-to-date Microsoft Windows 10 operating system including multiple antivirus solutions and advanced protection of Microsoft Office 365. Moreover, there was a need to simulate attacker infrastructure including own mail server, distribution point for malware and C&C server. Once everything was prepared, the client gave their approval, and the phishing campaigns with approximately of 1000 emails totally was executed. This security testing effort was conducted with emphasis on the actual state of the systems examined and no documentation by the client was provided.

Note: All information in this case study has been modified to maintain confidentiality of our client

PHISHING TEST PHASES

There are various approaches for phishing tests depending on available information provided by clients and their expectations. LIFARS Team in this case follows the approach of black-hat hackers with minimal or zero information provided by the client and with the objective of achieving a remote code execution. The main phases of this phishing test are listed below.

1. (Pre-engagement Interactions)
2. Information Gathering
3. Environment Setup
4. Campaign Scenarios and Custom Malware Development
5. Scheduling and Executing of the Campaigns
6. Exploitation
7. Reporting

INFORMATION GATHERING

We simulated an attacker targeting our client by implementing a spear-phishing campaign. For such campaigns it is important to gather specific types of information like email addresses of client's employees, names of managers with authority, information about used technologies and business. The gathered intel allows the attacker to be more precise when preparing scenarios that include message content, senders, recipients, and email attachments with malicious payloads.

As a first step we used publicly available services, search engines and leaked collections to gather email addresses and technology information.

ENVIRONMENT SETUP

After information gathering, the Environment needs to be prepared. This includes at least the following:

- Campaign Scenarios
- Public IP address (not blacklisted) and domain name suitable for prepared scenarios
- Email server which can send (and optionally receive) email messages for chosen domain
- Webserver for serving malicious or tracking content and keep tracks of clicked links in emails, optionally for collecting submitted credentials

- Depending on scenarios, malicious attachments or samples, tools which attackers use for initial compromising of victim, malware distribution points and Command & Control servers

For example, when creating the domain name, we used the same techniques as attackers often use, such as typo squatting and designing a plausible looking domain with different 1st level domain. We used a legitimate SSL/TLS certificate trusted by all major browsers on the webserver. Further, during the phishing test we didn't use any publicly available services to send emails because many of them were blacklisted by the client or would raise suspicious. Instead of that, we deploy own email server with enabled modern features and protections such as SPF, DKIM, DMARC, etc. With these settings, we were able to get very low score from spam checkers.

```
SpamAssassin Score: 0.7
Message is NOT marked as spam
Points breakdown:
 0.0 SPF_HELO_NONE          SPF: HELO does not publish an SPF Record
 0.1 DKIM_SIGNED            Message has a DKIM or DK signature, not necessarily
                            valid
-0.1 DKIM_VALID             Message has at least one valid DKIM or DK signature
-0.1 DKIM_VALID_AU          Message has a valid DKIM or DK signature from
                            author's domain
 0.8 FROM_FMBLA_NEWDOM28    From domain was registered in last 14-28
                            days
```

Figure 1: With very low spam score the message is not marked as spam

CAMPAIGN SCENARIOS AND CUSTOM MALWARE

We prepared three different scenarios reflecting the requirement of achieving malicious code execution by the victim, opening emails and/or attachments and clicking on links. We carefully chose actual hot topics related to most of the employees like their salaries and policies for remote work. This way recipients are more likely to open the email or click on the link; in some cases, even multiple times.

Our client relies on recent protections of Microsoft and some 3rd-party security products which provides very good level of protection to their infrastructure.

Outlook protection uses an extensive list of forbidden filetypes, and together with the up-to-date protections of Windows 10 (Microsoft Defender, SmartScreen, Security Zones) and Microsoft Office (Protected View, Active content and macros blocked by default) complex methodologies are required to create malware samples capable of delivering the "malicious" code to victim's computers. It also means that old-fashioned attachments like crafted Windows link (.lnk) files, or JavaScript (.js) inside of ZIP are blocked by at least one of these protection layers. Also, attachments with macro-enabled Office documents are very often detected by antiviruses, even with the obfuscated macros by automatic obfuscators or manual.

Despite, the high complexity, LIFARS' team of developers and malware analysts created three custom "malicious" samples based on our three scenarios. We developed an accounting program for salary verification, Excel form for remote work request (code execution was achieved without macros) and Help file with summary of changes in remote work policy. During the phishing test, all these three samples had very low detection ratio – by 0 or 3 antiviruses out of 69 on VirusTotal.

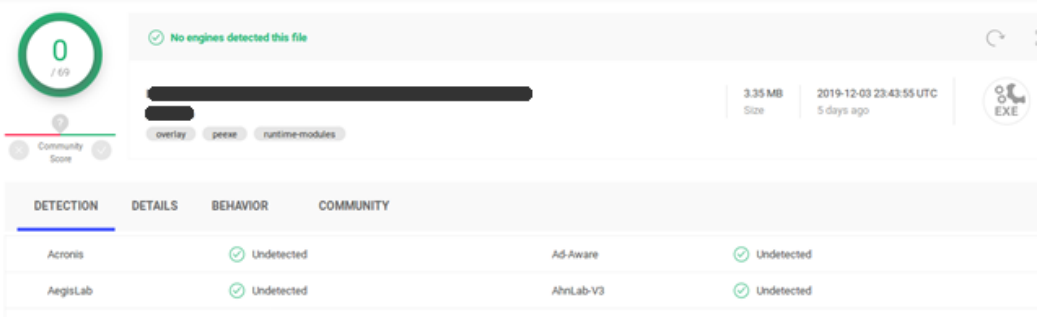

Figure 3: Antivirus Detections of Custom Malware Sample

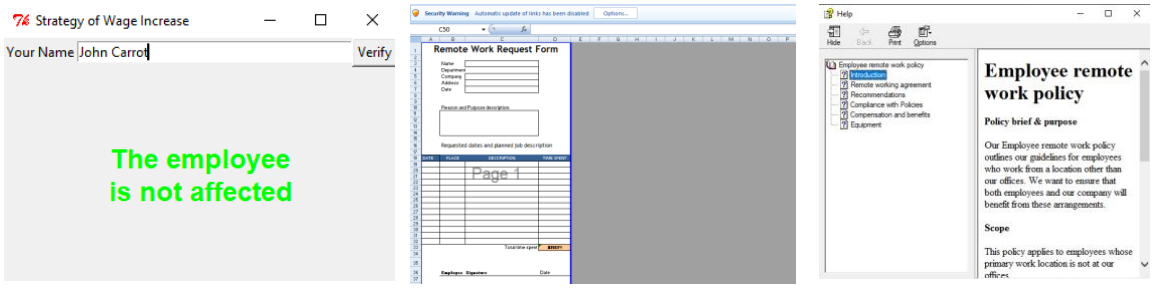

Figure 2: Custom Malware Samples delivered by email messages

One of these samples was suitable to be used as an email attachment directly, while other two could be shared from OneDrive. All these samples lead to execution of the code provided by "attacker"- in the form of executable file, or PowerShell commands downloaded from our webserver.

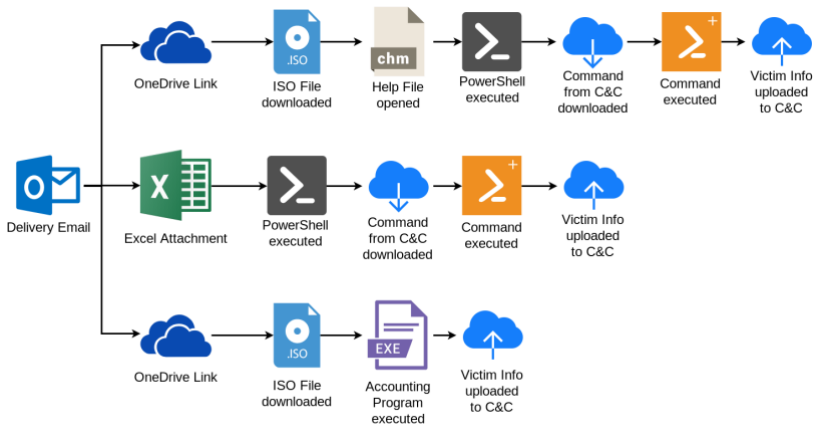

Figure 4: Scheme of Spear-Phishing Attack with Custom

SCHEDULING AND EXECUTION

During the first phase of the Phishing test we collected approximately 2000 email addresses in the three groups described above. After discussion with the client, the list was narrowed down to 1000 addresses with the requirement to exclude some email addresses. After the final list of recipients and scenarios was approved, a time slot for campaign execution was finalized. The day of operation we sent almost one thousands of emails, divided into three separate groups, and based on three distinct scenarios.

KEY FINDINGS

Out of 1000 recipients, 43 users opened our phishing emails. It is likely that this number is higher because emails can be opened without downloading external content – thus without connecting to our tracker.

With approximately, 800 successfully delivered emails, statistically at least 5% of recipients of these emails from our fake domain are prone to this typo squatting trick and they opened this phishing email, even when they were flagged with 'Unverified' keyword in mailboxes of the targeted company.

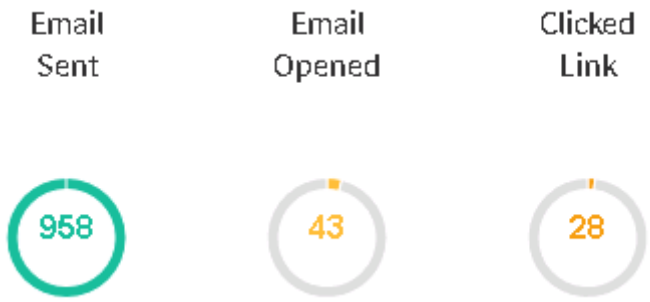

Figure 5: Overview of Campaign Stats

In two of the scenarios, we captured 23 users who clicked on the links with the intention of downloading and opening the file (salary check program or remote policy help). In the third scenario, we captured users' opening, downloading, and executing our payload on the attached Excel spreadsheet multiple times. A summary of all events is listed in following table.

“Malicious” file	**Delivery Method**	**Number of Clicks**	**Number of Executions**
Salary check program	OneDrive Link	5	0
Remote Work Request Form	Email Attachment	N/A	140
Remote Work Policy help	OneDrive Link	18	42

Further, some recipients replied to phishing emails and others had automatic replies enabled, consequently, client’s company information was leaked.

Additionally, recipients’ device information was captured when links were clicked, and emails opened. An analysis of the captured data revealed that some of the client’s employees used vulnerable iPhones.

time="2019-12-05T18:52:44+01:00" level=info msg="****** - - [05/Dec/2019:18:52:44 +0100] \"GET /****** HTTP/2.0\" 200 95 \"\" \"Mozilla/5.0 (iPhone; CPU **iPhone OS 12_4_1** like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148\""^M

time="2019-12-05T21:29:13+01:00" level=info msg="****** - - [05/Dec/2019:21:29:13 +0100] \"GET /****** HTTP/2.0\" 200 95 \"\" \"Mozilla/5.0 (iPhone; CPU **iPhone OS 12_4_1** like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148\""

These iPhones used iOS 12.4.1, at the time of the phishing test this version was outdated with known vulnerabilities. As described in a document released by Apple, the newer version iOS 12.4.2 resolved the security vulnerability CVE-2019-8641. The vulnerability could be misused by a remote attacker and potentially caused unexpected application termination or arbitrary code execution.

iOS 12.4.2

Released September 26, 2019

Foundation

Available for: iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, and iPod touch 6th generation

Impact: A remote attacker may be able to cause unexpected application termination or arbitrary code execution

Description: An out-of-bounds read was addressed with improved input validation.

CVE-2019-8641: Samuel Groß and Natalie Silvanovich of Google Project Zero

Figure 6: Vulnerability details

CONCLUSION

We used publicly available data to compile a list of users for this assessment. The users were then divided into multiple group based on the information collected about them. Three possible trustworthy, spear phishing scenarios were created targeting the user population. LIFARS then created three domains, one of which was used to send users spear phishing (which included the harmless malware but proved that the code was executed on the machines of the users). The spear phishing campaign hit multiple groups to decrease the probability of the Security Operations Center (SOC) detecting it as a campaign.

We found that multiple users had clicked the malicious links within the phishing emails and executed LIFARS' custom developed malware, which could result in a compromise of the organization or its part, if that was part of the exercise.

REPORTING

Key findings and concerns were outlined in the final report. Since, the phishing test was just one part of the Red Team Exercise, the final report also included Indicators of Compromise (IoC), like hashes of "malicious" samples, IP addresses and domain of distribution points and C&C servers. The client was also provided with captured data from the malware execution– usernames, hostnames and internal IP addresses, for better distinguish, who and where executed the malware sample. Further, the executive summary provided a brief summary of vulnerabilities discovered during this assessment and a schematic illustration of performed attacks and phishing campaigns. All issues were documented with recommendations given for resolution of each.

.