Targeted Email Attacks

A Detailed Analysis from FortiGuard Labs

Sophisticated attacks are increasingly designed to bypass organization-specific security controls. However there are established and emerging technologies, processes and services that can prevent, detect, and mitigate advanced attacks to greatly reduce the risk of an extended compromise and substantial data breach.

It is well documented in high profile data breaches, industry reports and analyst briefs that today's sophisticated attacks often begin with email and end in exfiltration of sensitive data. What are not always clear are the criminal steps that occur in between. The threat experts of FortiGuard Labs constantly analyze emerging threats to stay abreast of evolving attack techniques, share findings, update protections and drive innovation into Fortinet's security products. This paper includes a brief analysis from FortiGuard Labs of a real world evasive advanced threat – how it works and how a sandbox can help you identify it.

Lifecycle of an Advanced Attack

Step 1: Reconnaisance and Incursion

Sophisticated cybercriminals typically start with reconnaissance on the target organization. They then often craft a clever email, with a malicious link (or file) in it, and send the email to targeted recipients. Ideally, your email security- antispam, antiphishing, or anti-malware- will block the message. Generally, the message is a very simple and easily created (or modified) for just this one attack.

Further, you can see that in the following example the cybercriminal has embedded malicious code in a Word document that is socially engineered with the local langue file

Adding a Sandbox to Address Targeted Attacks

Many customers are increasing their defense with newer technologies like sandboxing (a secure, virtual environment in which code activity, and indeed the full threat lifecycle, can be dynamically analyzed), along with automated protection updates and incident response processes that trigger off of the findings of this tool.

name “Upcoming Event Schedule” along with a Microsoft Word icon to entice users to open it. It is designed to silently install itself behind the scenes, while a word document is opened, without any additional end user action required.

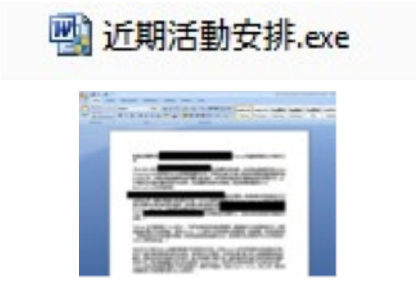


Figure 1– Social Engineering

Finally, its use of encrypted coding, as well as various stack calls, make it especially hard for static analysis to identify the malware.

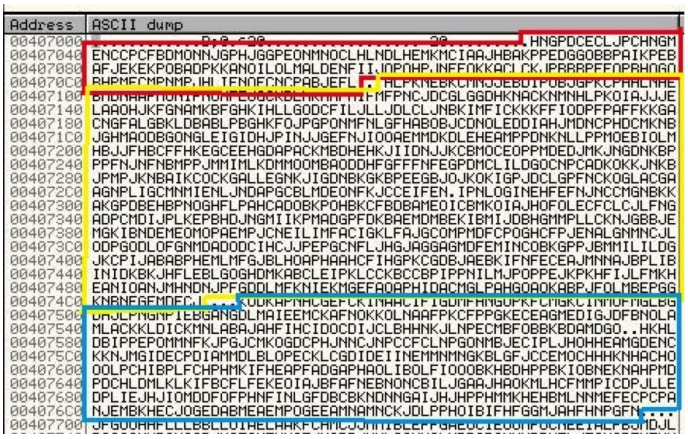


Figure 2– Encrypted Code

Step 2: Establish Communication and Begin Attack

If the target recipient is fooled into opening the attachment and it installs, traffic to a web site will establish communication. This is where your web filter may block the traffic. However in this case we can see that it only attempts to connect to two sites, which may very well have been created solely for this attack and for a limited duration. They were:

```
most.{Removed}an.com
1.170.11{Removed}
```

If your web filter is not aware of these new sites and able to establish a malicious rating in real-time, that malicious web site starts to attack your organization.

Step 3: Attempt to Exploit and Enter

The malicious web site will usually launch exploit attacks at the target to gain access to the system. This is where your intrusion prevention system (IPS) attempts to block the attack, but if it doesn’t: a tunnel is opened and malicious code delivered.

In this particular case, communication activity over Port 80 is encrypted using the following subroutine and completely hidden from IPS unless processor intensive SSL inspection is being utilized by the organization.

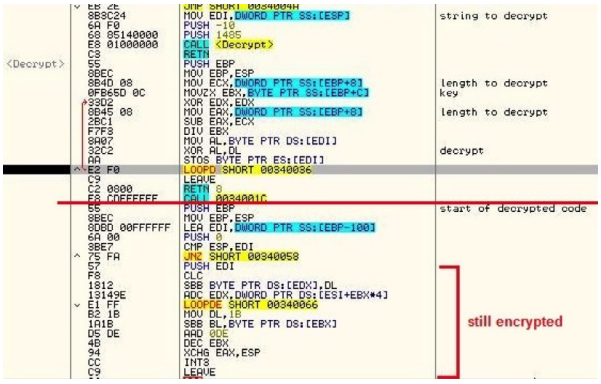


Figure 3- Encrypted Communication

Step 4: Malware Installation

With malicious code seeking entry, ideally your anti-malware will protect you, at the gateway or client device itself. But if it doesn’t the attacker gets executable code into your system.

In this case (as mentioned previously) the malicious code came directly with the email, it leveraged encryption and stack calls to defeat most static analysis and subsequent communications (and potential downloads) were encrypted to bypass network inspection.

Step 5: Lateral Movement and Data Exfiltration

Once the malicious code is running, it usually looks to access credentials, seek out sensitive data and collect/stage it within your organization.

In this case, among the commands the bot can send to the code on the machine is one to enumerate the drives or files.

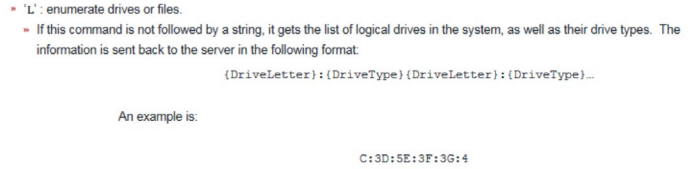


Figure 4– Exfiltration Commands

But in order to complete its mission, it needs to exfiltrate that data out to a command & control server. This is where your application control, IP reputation, botnet and other protections come into play. If they don't block this traffic: You are breached. And in this instance, encrypted communications circumvent these security controls without SSL Decryption in place.

Sandbox Analysis of an Advanced Attack

In response to sophisticated attacks like this one, many customers are increasing their defense with newer technologies like sandboxing (a secure, virtual environment in which code activity, and indeed the full threat lifecycle, can be dynamically analyzed), along with automated protection updates and incident response processes that trigger off of the findings of this tool. Here are some of the insights that sandboxing (from Fortinet's FortiSandbox) can provide.

First, FortiSandbox analysis uncovered advanced suspicious activity, including privilege modification, file creation and deletion of the invisible (to the end user) dropper.

Figure 5- File System Activity Uncovered by FortiSandbox

Second, evaluation of the subsequently dropped file flagged it as malicious.

Figure 6 – Analysis of the Subsequent Download by FortiSandbox

Third, even if the download itself had not been flagged, analysis of the network activity uncovered the encrypted traffic (itself a risk indicator) as well as the command and control site.

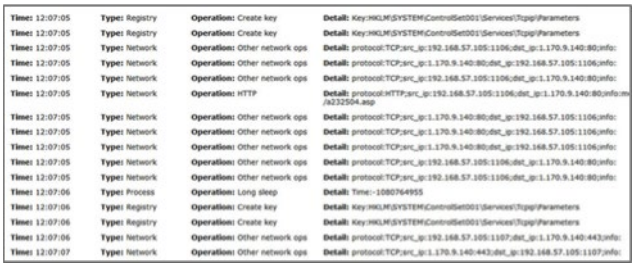


Figure 7- Network Behavior Identified By FortiSandbox

So this seemingly benign email message and attachment appears quite different when analyzed in a sandbox- which rated it 'high risk'.

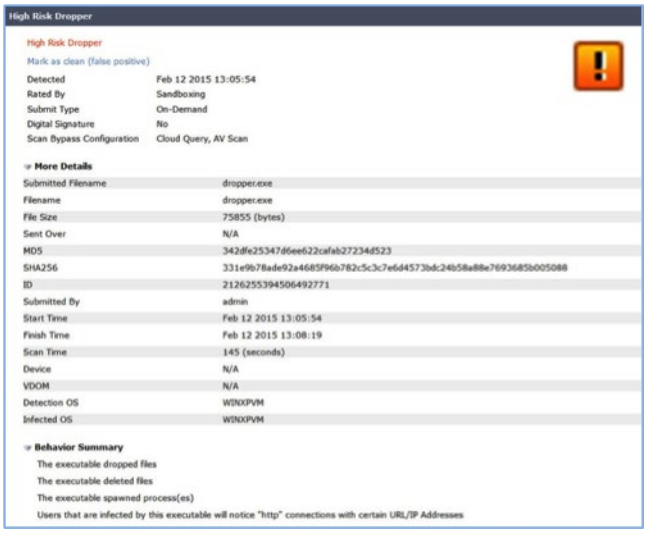


Figure 8– Sandbox Rating and Results

Organizations with this type of detailed information are able to take the following mitigating actions:

- Block this email sender IP from delivering any other messages to employees.
- Prevent communication with this command & control
- Quarantine recipient devices
- Confirm compromise and remove malicious files
- And more

Further, when the FortiSandbox is integrated with Fortinet's secure email gateway, FortiMail, this sandbox analysis can occur in real-time while the message is temporarily quarantined to await analysis can and ultimately blocked based on the result.

Finally, those organizations who choose to share the results of their sandbox analysis with FortiGuard Labs will receive automated updates to protection in the form of:

- Updated IP sender reputations
- New web site ratings used for web filtering
- New IPS rules and botnet detection to block command and control traffic
- Updated anti-malware detection for this and similar attachments
- And more as applicable

Conclusion

While attack techniques vary, FortiGuard researchers often see the following evasions techniques used to bypass traditional security technologies:

- Emails sent from compromised systems with a mixed reputation based on legitimate email during the day and bot controlled attacks at night
- Socially engineered messages, links and attachments to fool more security conscious end users
- Encrypted, compressed or password protected attachments to confuse static anti-malware inspection
- Fresh command & control sites that last only days or even hours thanks to fast flux and other techniques
- Encrypted communications to bypass IPS and other forms of network behavior analysis

Advanced Threat Protection

The most common technology considered for advanced threat protection in response to the evasion techniques above is sandboxing, which provides the dynamic analysis necessary to uncover today's targeted attacks, as well as the threat intelligence to thwart them. Further, sandboxing is increasingly available as an integrated component of existing infrastructure rather than a stand-alone solution operating independently. An integrated solution can speed up and automate the prevention and mitigation of attacks. In this case, Fortinet's FortiMail Secure Email Gateway and FortiSandbox provide such an integrated solution.

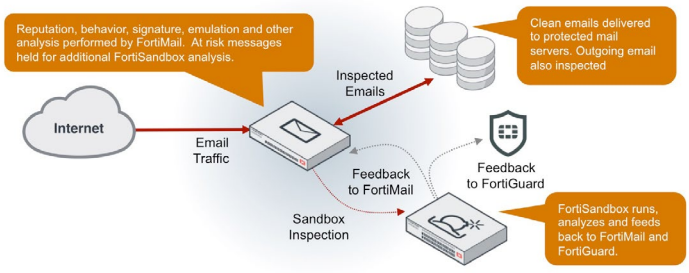
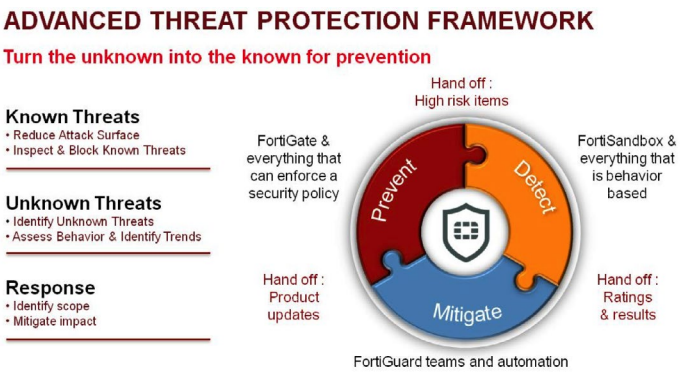


Figure 9– FortiMail- FortSandbox Integration

For more information on the FortiMail-FortiSandbox integration, read "Playing Safely in the Sandbox" http://www.fortinet.com/resource_center/whitepapers/fortimail-playing-safely-sandbox.html

Of course, adding the dynamic analysis of a sandbox is just one way to address the security risk posed by advanced threats. Fortinet recommends organizations consider a more cohesive approach designed to seamlessly align prevention, detection and mitigation of attacks for a continuous cycle of improvement. This approach is outlined in the Fortinet Advanced Threat Protection framework.

For more on this framework please visit http://www.fortinet.com/solutions/advanced-threat-protection.html.



Many thanks to FortiGuard threat researcher, Margarette Joven, for her tireless efforts uncovering new attacks and, in this case, sharing some of her detailed findings. (Please visit her blog post for even more detail.)

Thanks too for Jim Huber's views into how FortiSandbox helps customers uncover these attacks themselves.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480