Challenges of the Current and Evolving Threat Landscape

Brendan Griffin
Threat Intelligence Manager, PhishMe
A little about me

B.A. Philosophy, Birmingham-Southern College

Five years’ experience in malware analysis

Focus on the malware delivered by phishing email

Pony, NewGOZ, Dyre, Locky, TrickBot
Caveats, provisos, disclaimers

Citations are not endorsements—instead they are denotation of helpful examples.

Citations are not indictments—one misstep or error does not define a person or organization.

I have my biases but they’re not the law—I offer my perspective and welcome others’.

Information security is an evolving art and science—we’re all here to learn and stop the bad guys.
What do we mean by “threat landscape”

The attacker:

You mustn’t be afraid to dream a little bigger, darling.
What do we mean by “threat landscape”

And where it leaves the defender:
What do we mean by “threat landscape”

Composite of techniques, tools, and methodologies

Combined with the existing vulnerabilities that are available to attackers

Some attacker preferences, proclivities, and "feelings"

The things that seem like a huge deal, might not always be as important as they seem
What’s happened this year

- Shadow Brokers leaks (started 2016)
- Locky, Jaff, Dridex all distributed by Necurs botnet
- Google Docs Gmail “worm” hits the Google cloud
- WannaCry, notPetya create global crises
Shadow Brokers setting the stage

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANANAGLEE</td>
<td>6 items</td>
<td>Folder</td>
</tr>
<tr>
<td>BARGLEE</td>
<td>1 item</td>
<td>Folder</td>
</tr>
<tr>
<td>BLATSTING</td>
<td>7 items</td>
<td>Folder</td>
</tr>
<tr>
<td>BUZZDIRECTION</td>
<td>2 items</td>
<td>Folder</td>
</tr>
<tr>
<td>EXPLOITS</td>
<td>8 items</td>
<td>Folder</td>
</tr>
<tr>
<td>OPS</td>
<td>6 items</td>
<td>Folder</td>
</tr>
<tr>
<td>SCRIPTS</td>
<td>33 items</td>
<td>Folder</td>
</tr>
<tr>
<td>TOOLS</td>
<td>15 items</td>
<td>Folder</td>
</tr>
<tr>
<td>TURBO</td>
<td>2 items</td>
<td>Folder</td>
</tr>
</tbody>
</table>

Equation Group Cyber Weapons Auction - Invitation

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!
Shadow Brokers setting the stage

```
specials
  | etch-0.dll
  | etchCore-0.x64.dll
  | etchCore-0.x86.dll
  | eteb-2.dll
  | etebCore-2.x64.dll
  | etebCore-2.x86.dll
  | Eternalblue-2.2.0.xml
  | Eternalblue-2.2.0.exe
  | Eternalblue-2.2.0.fb
  | Eternalchampion-2.0.0.xml
  | Eternalchampion-2.0.0.exe
  | Eternalchampion-2.0.0.fb
```

Kevin Beaumont @GossiTheDog · Apr 14

Rephlying to @GossiTheDog

ETERNALBLUE and ETERNALCHAMPION are both SMB2 and SMB1 exploits
virustotal.com/en/file/85b936... virustotal.com/en/file/ce7345...

Kevin Beaumont @GossiTheDog

ETERNALBLUE exploit also works against 2008 R2, as per @hackerfantastic. SMB exploit, another zero day.

10:36 AM · 14 Apr 2017
Dridex, Locky, Jaff, etc.

![Graph showing the number of distinct attacks for Dridex, Locky, and Jaff from January 2017 to July 2017.](image-url)
Dridex, Locky, Jaff, etc.

- **Locky**
- **Dridex**

The chart shows the number of distinct attacks from January 2016 to July 2016. The peak for Locky was in March 2016, while Dridex had significant spikes in March and May 2016.
Dridex, Locky, Jaff, etc.

What's the deal?

Lower frequency, but different techniques

Retooling, updating, iterating

Thinking about "What does phishing look like?"
Dridex, Locky, Jaff, etc.

- Familiar Office documents with macros were a hallmark for distribution of these malware tools
Dridex, Locky, Jaff, etc.

- Simply changing up the look and feel makes a huge difference
- Defies the expectations set by security and awareness professionals
Moving beyond the macro

- For a real departure, though, look to Ursnif
- OLE package abuse writes a script application to disk
Google Drive, Gmail "worm"

- Demonstrated the intersection of phishing and cloud services
- Malicious code was not executed on the endpoint
- Nor was it designed to create a fake login page
Google Drive, Gmail ”worm”

- Common message but with a distinctive twist
- Rather than running code on the endpoint, the malware took advantage of cloud service application permissions
Attacking the cloud

• The cloud provides mission-critical services for many enterprises
• But it’s still just computers
• Similar protections should be extended

• Two-factor authentication, telemetry, preparation for common attack vectors
WannaCry’s legacy

- Caught the world by surprise using ETERNALBLUE
- Pretty unsuccessful as a ransomware tool
- Very successful as a worm
Its strength and its weakness

Highly virulent thanks to SMB exploitation

But also highly sensitive to the sinkholing of a single resource

Sample I found scans SMB after dropping WannaCry. Can anyone confirm it’s the same thing? P2P spreading ransomware would be significant.

#WannaCry propagation payload contains previously unregistered domain, execution fails now that domain has been sinkholed.
Just bad for business

small number of Bitcoin wallets + global scope = focus of authorities everywhere
focus of authorities everywhere = difficulty in extracting financial gain
Industry springs into action

- Cutting off communication often helps slow or stop an attack
- Impulse to block everything related to the ransomware’s infrastructure was seemingly well-founded

However, in this instance it created a disadvantageous scenario for defenders

Alan Woodward @ProfWoodward
Oh crap! Whoever maintains the UK ISP blacklist needs to act now to remove the wannacry domain - you’re doing more harm than good

12:02 PM - 13 May 2017

David Redekop @DRtheNerd
If [redacted] is blocking the killswitch domain, it’s unintentionally allowing #WannaCry to continue?

12:31 AM - 13 May 2017

Tom Cross @clarius_
I’m seeing multiple security vendors/solutions that are blocking access to the @MalwareTechBlog WannaCry killswitch domain. This is harmful.

8:12 AM - 13 May 2017
NotPetya’s legacy

Iterated on WannaCry’s tools for success

Intended to disrupt and destroy instead of extract financial game

Showed that lessons are hard-earned and hard-learned
High-impacts and supply chains

- Striking first in Ukraine via software supply chain attack
- Quickly spread within networks using SMB exploits and all the pentester’s tricks
- Password reuse, domain admin stuff, etc
RUMINT and you

- Speculation about phishing as the infection vector spread quickly
- Rumor Intelligence
- One set of emails was highlighted repeatedly and with circular citation of the same sources

- But the rumors were not true—those emails delivered Loki Bot, not NotPetya

Hello,

We sent you an email last week Thursday been the 22nd of June 2017, to this email address [redacted]. Until this time we have not received your quote as requested in that email. We are resending you the same PO as attached in this email, please Send us your best price offer for the attached PO's, we need to make new orders for this new week. Please kindly view the attached order list and send us Quotation. Thanks

Best Regards
Christian Malcharzik
Sales Manager

<table>
<thead>
<tr>
<th>Attached document name</th>
<th>Attached document MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order-20062017.doc</td>
<td>415fe69bf32634ca98fa07633f4118e1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loki Bot payload location</th>
<th>Loki Bot Command and Control location</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxxp://french-cooking[.]com/myguy.exe</td>
<td>hxxp://coffeinoffice[.]xyz/cup/wish.php</td>
</tr>
</tbody>
</table>
RUMINT and you

- Blocking the wrong, but still active threat
- False sense of security leading to inaccurate triage
- Allocation of resources on any given day is already difficult
- Allocation of resources in a crisis can be even more challenging
What does this all mean for the enterprise?

- Attackers have (and will continue to) change the threat landscape
- The attacker skill gap is closing and will continue to close
- How can you identify the "sophisticated" attacks when they're all sophisticated (or unsophisticated)?
- What does a "next-generation" of ransomware look like?
Changing the threat landscape

• Nothing happens in a vacuum and threat actors learn from each other
• The *zeitgeist* created by high profile leaks like Shadow Brokers may be linked to the increased use of exploitation by attackers

• Remember the email delivering Loki Bot on the same day as NotPetya--delivered an RTF document exploiting CVE-2017-0199

```
Hello,

We sent you an email last week Thursday been the 22nd of June 2017, to this email address [redacted]. Until this time we have not recieved your quote as requested in that email. We are resending you the same PO as attached in this email,please Send us your best price offer for the attached PO's, we need to make new orders for this new week. Please kindly view the attached order list and send us Quotation. Thanks

Best Regards
Christian Malcharzik
Sales Manager
```
Closing the attacker skills gap

Sometimes it’s a promethean effort for a “hacktivist” of sorts like Shadow Brokers

Other times it’s just clever coding and software development skill

Either way the result is less-skilled attackers doing less work to get their hands on powerful tools
Muddy waters of attribution

When every attacker has top-tier tools, how do you know if it's script kiddies or nation-state?

Your own strengths and weaknesses help determine if that distinction matters.

Leverage your community--that means vendors, too.

Understanding the scope and reach of what's happening can help you keep perspective.

Triage first, ask questions later.
What does a “next-generation” ransomware look like?

This?
What does a “next-generation” ransomware look like?

This?
Maybe.
What does a “next-generation” ransomware look like?
What does a “next-generation” ransomware look like?
What does a “next-generation” ransomware look like?

If the ransom amount is not paid by the final deadline shown above, these three things will happen -

1. Your photos, videos, and financial information will be made available online.
2. If we find any nude photo or video on your system, it will be sent to your contacts and will be uploaded to porn websites as well.
3. All of your data will be deleted, and you won’t be able to recover it after that.
What does a “next-generation” ransomware look like?

- Pop culture gave us one image in *Black Mirror*’s “Shut Up and Dance”
- Karo ransomware gives us a (kind of) real world example of privacy for ransom
- Spora paints a picture of a business model built upon helping victims be customers
So now what?
So now what?

first rule.
So now what?

*first* only rule.
So now what?

DON'T PANIC
So now what?

Be real and realistic about what matters to your organization

Know not thy enemy, but instead their tactics, techniques, and procedures

Set goals for your own unique, holistic, comprehensive, and agile defense
Be real and realistic

Brainstorm, research, and do your best to understand how an attacker might hit you.

Understand what problems can be solved easily and which are more difficult.

It's easy to defend against the things you understand--try to understand more.

Assess ROI on security solutions.
So now what?

Prepared / Condition Users

Promote User Reporting

Triage

Analyze

Respond

Existing Security Solution Set

Intelligence

Internal Assessments

Community Engagement
Read more about my work and that of my colleagues

phishme.com/blog
twitter.com/phishmeintel
Questions?
Discussion.