Targeted Attacks
A Shift from Economic Espionage to Politically Motivated Sabotage and Subversion

Kevin McPeak, CISSP, ITILv3
“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, *The Art of War*
Threat Landscape
A fundamental shift...

Old Motivation
Hacking
Cyber Crime
Cyber Espionage
Cyber Warfare
Top Messages:

- Big Numbers in 2016
- Targeted Attacks Shift from Economic Espionage to Politically Motivated Sabotage and Subversion
- Attackers Weaponize Common IT Tools
- Email Became The Weapon of Choice for 2016
- North Korea Had $1 Billion in Their Sights, Got Away With $94 Million
- Banner Health Breach
- WannaCry Deep Dive
### Big Numbers

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total breaches</strong></td>
<td>523</td>
<td>1,211</td>
<td>1,209</td>
</tr>
<tr>
<td><strong>Breaches with more than 10 million identities exposed</strong></td>
<td>11</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total identities exposed</strong></td>
<td>128</td>
<td>548B</td>
<td>1.8B</td>
</tr>
<tr>
<td><strong>Average identities exposed per breach</strong></td>
<td>805K</td>
<td>466K</td>
<td>927K</td>
</tr>
</tbody>
</table>

In the last 8 years more than 7.1 billion identities have been exposed in data breaches.
## Big Numbers

### Email threats, malware, and bots

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam rate %</td>
<td>1 in</td>
<td>1 in</td>
<td>1 in</td>
</tr>
<tr>
<td>Phishing rate</td>
<td>965</td>
<td>1,846</td>
<td>2,596</td>
</tr>
<tr>
<td>Email malware rate</td>
<td>244</td>
<td>220</td>
<td>131</td>
</tr>
<tr>
<td>New malware variants</td>
<td>275M</td>
<td>300M</td>
<td>347M</td>
</tr>
<tr>
<td>Number of bots</td>
<td>93.0M</td>
<td>96.6M</td>
<td></td>
</tr>
</tbody>
</table>
Big Numbers
Big Numbers

Internet of Things

2 minutes: time it takes for an IoT device to be attached

Speed of attack

Number of attacks against Symantec: reported per hour

Jan 2016

Mar 2016
Is This Ladder a Threat?
Is This Ladder a Threat?
Living off the Land

Attacker are using what’s available to attack us

- These tools are ubiquitous
- These tools are easy to use for malicious purposes
- These tools don’t arouse suspicion, and can be difficult to determine intent.

“living off the land” means using whatever tools are on hand, such as word documents, email, powershell, other legitimate network administration software and operating system features to attack. Its taking advantage of what users have in their environment. Even IoT devices have become a tool for attackers. Living off the land works to the attackers advantage because the tools are ubiquitous, most victims are running these programs, or can run them. They are easy to use for malicious purposes, much easier than finding and exploiting Zero-day vulnerabilities and writing sophisticated malware. And they allow attackers to hide in plain sight. End-users and IT expect these tools to be on a machine. And the intent of the tool, that it is being used for harm, can be hard to determine.

One thing we will see throughout the ISTR is examples of how these tools have been used and abused by attackers. It is a part of almost every other trend we’ll talk about today.
Cyberattacks involving sabotage have traditionally been quite rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in Ukraine in January and again in December, attacks which also resulted in power outages. Meanwhile the disk-wiping Trojan Shamoon reappeared after a four year absence and was used against multiple organizations in Saudi Arabia.

DeepSight Intelligence has observed several companies in Saudi Arabia potentially targeted by the attack:
- A petrochemical firm
- An international holding company
- An electronic payment system company
- An international technology company
- Two financial organizations

Shamoon was first used in attacks against the Saudi Arabian energy sector in 2012, a new variant (W32.Disttrack.B) was used against targets in Saudi Arabia in November 2016 and January 2017. In the first wave of new attacks, the malware was configured to launch its disk-wiping payload at 8:45pm local time on Thursday, November 17. The Saudi Arabian working week runs from Sunday to Thursday. Thus, the attack was timed to occur after most staff had gone home for the weekend in the hope of reducing the risk of discovery before maximum damage could be caused.

In Jan 2017, The Greenbug group, which also targets the Middle East but predominately Saudi Arabia, has been potentially linked to the Shamoon malware. Greenbug uses its custom Modor remote access Trojan to steal credentials from compromised organizations in the aviation, energy, government, investment, and education sectors.

On 23 January 2017, cyber attacks using the Shamoon disk-wiping malware (detected by Symantec as W32.Disttrack and W32.Disttrack.B) were carried out simultaneously across several different industries and companies in Saudi Arabia including the aviation, biochemical, steel, and contracting and construction sectors.

The Shamoon malware was configured with passwords that appeared to have been stolen from the targeted organizations. These passwords were likely used to allow the malware to spread across an organization’s network.

The attacks were likely politically motivated. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three year-old Syrian refugee who drowned in the Mediterranean in 2015.

A number of attacks against Ukraine involving the use of disk-wiping malware in 2016. The attacks were linked to what is likely a Russian cyberespionage group. This group is known as Sandworm and involved a highly destructive Trojan (Trojan. Distrack). Attacks in late 2015 and early 2016 hit the energy sector in Ukraine, with the latter being linked to power outages in the country.

The malware was designed to run on Linux computers and, if run, rendered them unusable by encrypting key operating system files. Once the encryption has finished, it displayed a message demanding a ransom of 222 Bitcoin (approximately US$210,000 at the time of the attacks). Paying the ransom would not decrypt the affected files, with the encryption keys generated on the infected computer not saved locally or to a command and control (C&C) server. The malware was likely disguised as ransomware in order to trick victims into not investigating attacks thoroughly.
### Notable Target Attack Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Year</th>
<th>Description</th>
<th>Initials / Geol.</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Sandworm** | 2014 | **Tools, Tactics, & Procedures (TTP)** | Athens / Straddle, NY, LAT | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** include new webshell attacks.
| **Hoesefly** | 2011 | **Tools, Tactics, & Procedures (TTP)** | Athens / Equatorial | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** included new webshell attacks.
| **Fritillary** | 2012 | **Tools, Tactics, & Procedures (TTP)** | Athens / Cayman, Ottawa, North Carolina, Capitol, LAT | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** targeted webshell attacks.
| **Strider** | 2013 | **Tools, Tactics, & Procedures (TTP)** | Athens / Brazil | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** targeted webshell attacks.
| **Swallowtail** | 2017 | **Tools, Tactics, & Procedures (TTP)** | Athens / Taipei, TP, Tokyo, Berlin, Delhi | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** targeted webshell attacks.
| **Suckfly** | 2014 | **Tools, Tactics, & Procedures (TTP)** | Athens / Bahrain | Tools & Tactics analysis, UVH, malware, & remote code execution.
|           |      |             |                  |       | **Recent activities** targeted webshell attacks.

*Images in the document are not provided.*
Notable Target Attack Groups

**Cadelle**
- **Tools:** TTPs, & procedures
- **Target categories:** & regions
- **Recent activities:**
- **Tools:**
- **Target categories:** & regions
- **Recent activities:**

**Buckeye**
- **Tools:** TTPs, & procedures
- **Target categories:** & regions
- **Recent activities:**
- **Target categories:** & regions
- **Recent activities:**

**Appleworm**
- **Tools:** TTPs, & procedures
- **Target categories:** & regions
- **Recent activities:**
- **Tools:**
- **Target categories:** & regions
- **Recent activities:**

**Tick**
- **Tools:** TTPs, & procedures
- **Target categories:** & regions
- **Recent activities:**
- **Tools:**
- **Target categories:** & regions
- **Recent activities:**
As we do every year in the ISTR, we review the most notable targeted attack incidents that happen in the year. These attacks are predominately cyber-espionage. Not in 2016. The shift in 2016 is that targeted attacks are being used for sabotage and subversion.

To paraphrase Clausewitz, cyber-attacks are politics by other means.

We’ll look at examples of attacks representing both sabotage and subversion.
The US intelligence community’s report into the DNC data thefts and subsequent public disclosures assessed that they were part of an influence campaign conducted by the Russian Government aimed at the 2016 US presidential election. This is a group we have been tracking for over a decade. Their previous attacks were classified as cyber-espionage. So this is a shift from previous attacks.

The US intelligence community reports that the attacks were an attempt to influence the US election and also concluded that the campaign would have been seen as a success in Russia and that these activities will likely be used to inform future influence operations.

Given the proven potential for sowing discord and confusion, there is a strong likelihood that these tactics may be used again in a bid to destabilize other countries. France and Germany are both holding elections this year and already Bruno Kahl, the head of Germany’s foreign intelligence service, has said the same kind of attacks have already begun against Germany. “We have evidence of cyberattacks that have no other purpose than triggering political uncertainty,” he said. “The perpetrators are interested in delegitimizing the democratic process as such, no matter who that subsequently helps.”

These types of attacks reflect a broader shift towards highly-publicized, overt campaigns.
2016 Banner Health Breach

Highlights

• Compromised PoS system
  – Credit Card data stolen

• Infiltrated the primary Data Center
  – Doctor’s and other hospital employee’s personal data stolen

• Made their way into the Electronic Medical Records database
  – 3.7M Patient Records Compromised

• This is their 2nd breach in 2 years
  – SSN on 55k Mailers
Increased use of cloud services also helps facilitate a trend where attackers opting to “live off the land” instead of developing their own attack infrastructure. Let’s look at the example of John Podesta. In 2016 John Podesta was the Chairman of the Hillary Clinton presidential campaign.
In what may be the world’s most famous phishing attack, the Gmail account of John Podesta was compromised. According to the FBI, this spear-phishing email sent to campaign chairman John Podesta’s email account on March 19, 2016.

The email was crafted to appear as though it originated from an official Gmail administrative account. The branding looks consistent (Google logo, shield logo). The email is addressed to the recipient (not “Dear Sir”). The English is not broken. It appears to be very well crafted.
Anatomy of a Targeted Phishing Attack

Best practice for end-users is to hover their mouse over a link to view the real URL of a link. This used shortened URL which obfuscated a malicious URL.

Even if the end-user could length the URL the true domain is obfuscated. A first glance the domain appears to be myaccount.google.com. But if you look closely you can see that the actual domain is myaccount.google.com-securitysettingpage.tk That’s not Google. But it’s a lot more social engineering than a cyber-criminal puts into a phishing attack.
Anatomy of a Targeted Phishing Attack

- The login page looks identical to the actual login page (HTML was cloned).
- Once the user submits the username/password combination, it doesn’t matter what happens next.
- Typically, the phishing page redirects users back to Google.com.

Once clicked, the victim is directed to a fake password reset page masquerading as a legitimate Gmail account reset page. The login page looks identical to the actual login page (HTML was cloned). Once the user submits the username/password combination, it doesn’t matter what happens next.

Typically, the phishing page redirects users back to Google.com.

No malware or exploits were needed to perform the attack. Instead, simple social engineering was used to obtain a password.
Anatomy of a Targeted Phishing Attack

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this be done ASAP.

But luck, or a typo also played its part in the success of this attack.

Mr. Podesta asked about the email he received. He didn’t just click it. His assistants forward a letter from their IT. You can see that the advice is good. He was urged to change his password. HE was urged to use 2-factor authentication. All good.

He was given the correct URL to go to.

But the message contained a single typo. The word NOT was left out. This changed the meaning of the message. And Mr. Podesta clicked on the link in the email.
The Outcome of a Targeted Phishing Attack

The Podesta Emails

WikiLeaks series on deals involving Hillary Clinton campaign Chairman John Podesta. He Podesta is a long-term associate of the Clinton and was President Bill Clinton’s Chief of Staff from 1996 until 2001. He Podesta also owns the Podesta Group with his brother Tony, a major lobbying firm and the Chair of the Center for American Progress (CAP), a Washington DC-based think tank.

Read The Podesta Emails, Part 1: John Podesta and The Uranium One Story

Search by Terms in Email  Search by Attached Filename  Search by Email-ID
French Elections: Targeted Phishing Attack

- Macron campaign under heavy Targeted Attack
- Forward (creative) thinking may have saved his campaign
- 44 hour candidate and media blackout didn’t hurt either
Cyber Bank Heists

North Korea Had $1 Billion in Their Sights, Got Away With $94 Million
The methods used in this attack, in particular the in-depth knowledge of the SWIFT systems and the steps taken to cover tracks, are indicative of highly proficient actors. This was an incredibly audacious hack, and was also the first time strong indications of nation state involvement in financial cyber-crime had been observed.

Symantec’s analysis of the malware (Trojan.Banswift) used in the attack on the Bangladesh bank found evidence of code sharing between this malware and tools used by Lazarus – which the FBI claims has links to the North Korean government. The Lazarus group was associated with the infamous Sony hack in 2014, and has been linked to a string of attacks against the US and South Korea since 2009.

This same group was also linked to two other bank heists targeting banks that make transfers using the SWIFT network, though the SWIFT network itself was not compromised in any of these attacks.
The criminals exploited weaknesses in the Bangladesh bank’s security to infiltrate its system and steal the bank’s SWIFT credentials, which allowed them to make the fraudulent transactions. The criminals then used malware to cover their tracks. The malware was able to doctor the Bangladesh bank’s printed transaction confirmation messages in order to delay discovery of the fraud. The attackers also carried out the attack at the start of a long weekend in Bangladesh, to further reduce the chance of the thefts being discovered.

Using the stolen SWIFT credentials from the Bangladesh bank, the criminals made several transfer requests to the Federal Reserve Bank of New York for it to transfer the Bangladesh bank’s money, primarily to locations in the Philippines and Sri Lanka. Four requests to transfer a total of $81 million to entities in the Philippines successfully went through, but a request to transfer $20 million to a non-profit foundation in Sri Lanka raised suspicions because foundation’s name was spelled incorrectly. This led to the transfers being suspended and clarification being sought from Bangladesh, which uncovered the fraud. However, by then the $81 million had disappeared, primarily into accounts related to casinos in the Philippines.

Most of that $81 million remains unrecovered, however, $15 million was returned by a casino in the Philippines to the Bangladesh Central Bank in November.

There were about 30 more transactions, totaling up to $850-870 that were blocked before they went through, which could have made the total loss almost 1 billion dollars.
This same group was also linked to heists targeting banks that make transfers using the SWIFT network, though the SWIFT network itself was not compromised in any of these attacks.

Vietnam’s Tien Phong Bank revealed that it had intercepted a fraudulent transfer of more than $1 million in the fourth quarter of 2015. Research by Symantec also uncovered evidence that another bank was targeted by the same group in October 2015. A third bank, Banco del Austro in Ecuador, was also reported to have lost $12 million to attackers using fraudulent SWIFT transactions, although no definitive link could be made between that fraud and the attacks in Asia.

Symantec has evidence that these attacks targeted at least 30 other countries.

Symantec believes the Lazarus group may have reappeared in 2017 with further attacks against financial institutions.
WannaCry Ransomware
Generating Significant Global Attention
WannaCry Ransomware
Basics of the Attack

- Microsoft announces SMB vulnerability and patch within MS17-010
- Shadowbrokers release EternalBlue in their data dump which exploits this Microsoft SMB vulnerability
- WannaCry is seen in the wild and initial compromise vector unknown
- WannaCry encrypts files for ransom on host and propagates to other unpatched/unprotected hosts

Remember Shadow Brokers is the group that hacked Equation and stole their tools. In addition to the

Symantec has uncovered two possible links that loosely tie the WannaCry ransomware attack and the Lazarus group:

**Co-occurrence of known Lazarus tools and WannaCry ransomware:** Symantec identified the presence of tools exclusively used by Lazarus on machines also infected with earlier versions of WannaCry. These earlier variants of WannaCry did not have the ability to spread via SMB. The Lazarus tools could potentially have been used as method of propagating WannaCry, but this is unconfirmed.

**Shared code:** As tweeted by Google’s Neel Mehta, there is some shared code between known Lazarus tools and the WannaCry ransomware. Symantec has determined that this shared code is a form of SSL. This SSL implementation uses a specific sequence of 75 ciphers which to date have only been seen across Lazarus tools (including Contopee and Brambul) and WannaCry variants.

Symantec has “Medium Confidence” in regards to Appleworm and WannaCry connections.
Symantec's Timeline of WannaCry
Symantec Blocked 22M Attempted Attacks Over Hundreds of Thousands of Endpoints

Microsoft announces vulnerability MS17-010 and releases patch

WannaCry is first seen in the wild

Symantec delivers protection to block SMB exploitation of MS17-010 including blocking for EternalBlue for SEP14, SEP12 and Norton

Microsoft announces vulnerability MS17-010 and releases patch

Continuous Protection
- Critical Systems Protection (CSP)
- Data Center Security (DCS)
- Cloud Workload Protection (CWP)
- IT Management System (IMS)
- Control Compliance Suite (CCS)
- Malware Analysis / Cynic
- MSSP
- Cyber Security Services

Symantec delivers further updates to protect against potential new variants for SEP14, SEP12 and Norton

Symantec delivers further updates to protect against potential new variants for SEP14, SEP12 and Norton

ShadowBrokers release EternalBlue

Symantec Endpoint Advanced Machine Learning and Norton automatically block most variants of WannaCry

Symantec Global Intelligence Network instantly adapts providing protection to SEP14 and Blue Coat ProxySG

March 14
April 14
May 2
May 12 – 1AM Central US
May 12 – 3PM Central US

Copyright 2017, Symantec Corporation
Appleworm / Lazarus Ties

- Appleworm and WannaCry linked infection activity
- (same server/time/code)

<table>
<thead>
<tr>
<th>Sample #</th>
<th>MD5</th>
<th>Identification</th>
<th>First Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6851b87b53d27b974e3e0410b97b7811e</td>
<td>WannaCry dropper, drops Samples 2 and 3</td>
<td>8 May 2017</td>
</tr>
<tr>
<td>2</td>
<td>5b66b605e3e0410b97b7811e0410b97b7811e</td>
<td>WannaCry payload, dropped by Sample 1</td>
<td>28 April 2017</td>
</tr>
<tr>
<td>3</td>
<td>5179052637526325126325126325126325126</td>
<td>WannaCry payload, dropped by Sample 1</td>
<td>28 April 2017</td>
</tr>
<tr>
<td>4</td>
<td>707fe9b597e1516566652f9212e4537</td>
<td>WannaCry dropper, drops Sample 3</td>
<td>5 April 2017</td>
</tr>
<tr>
<td>5</td>
<td>59815ca9f4727275387f9200000666c</td>
<td>WannaCry payload, dropped by Sample 1</td>
<td>5 April 2017</td>
</tr>
<tr>
<td>6</td>
<td>68ec24550b5682412169f75644c863e</td>
<td>Brandbot</td>
<td>16 September 2011</td>
</tr>
<tr>
<td>7</td>
<td>6e1290877f3c5995050738540e338b</td>
<td>Malware containing worm functionality</td>
<td>5 February 2017</td>
</tr>
<tr>
<td>8</td>
<td>68ec7056bb78a9595265c2567</td>
<td>Malware containing worm functionality</td>
<td>5 April 2017</td>
</tr>
</tbody>
</table>

Table 1. WannaCry and collocated samples from three hosts
Appleworm / Lazarus Ties

- **Shared Command & Control Infrastructure**
  - 58.185.197.210
  - 84.92.36.96
  - 203.69.210.247
  - 184.74.243.67
  - 196.45.177.52 (sample 9)

![Diagram showing C&C infrastructure and related malware](image)

Table 2. Malware connected to Sample 8
Appleworm / Lazarus Ties

• **Shared Code**
  • Unusual custom implementation of the TLS/SSL protocol
  • Specific sequence of 75 ciphers
  • This implementation of TLS/SSL has only been observed in Appleworm tools including Contopee

<table>
<thead>
<tr>
<th>Sample #</th>
<th>MD5</th>
<th>Identification</th>
<th>Internal Compile Date</th>
<th>First Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>6c37451933a4e97026e7a32e15b3b3c</td>
<td>WannaCry</td>
<td>8 February 2017</td>
<td>10 February 2017</td>
</tr>
<tr>
<td>19</td>
<td>ac31b2e869f721174f4f43f82f3488</td>
<td>Contopee</td>
<td>20 February 2015</td>
<td>27 December 2016</td>
</tr>
</tbody>
</table>

Table 3. An early WannaCry sample that shares code with Appleworm malware (e.g., Contopee)
Thank You!

Kevin McPeak, CISSP, ITILv3

kevin_mcpeak@symantec.com
@kevin_mcpeak