TOMORROW'S NEWS IS TODAY'S INTEL

JOURNALISTS AS TARGETS AND COMPROMISE VECTORS

Shane Huntley  Morgan Marquis-Boire
@shanehuntley @headhntr
Overview

● Why journalists

● The threats we see

● Regional Variation

● What we can do
Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now.
US Constitution

Amendment I

Congress shall make no law ... abridging the freedom of speech, or of the press;
Article 19 of the Universal Declaration of Human Rights adopted in 1948 states simply that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers."
Watergate and Deep Throat

“Holding the powerful to account”

Watergate Scandal took down a President

Primary source,

“Deep Throat” secret for 30 years
The second oldest profession

Espionage, Spying and secrets

Who has great contact networks and traditionally poor operational security procedures?

Declassified documents show NSA spying on New York Times journalist Tom Wicker back in the 70’s under Project Minaret
Welcome to Today
Threats and Attacks
"In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google....

...this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors--have been similarly targeted."

-- Official Google Blog
The Media Giant

Fake questionnaire from Beijing News Office

Govt malware of .cn origin.

Opened by 10 employees.

Unfortunately, they believed anti-virus would protect them.
The Newspaper

National daily paper

Active compromise

Commercial government-only tools

European vendor
FINFISHER™: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS
IO: State Security Investigation Department  
Cairo  
Egypt

OFFR NO. 0610 - FF-GUK-061  
DATE Tuesday June 29, 2010  
CUSTOMER ID EGY-SSD  
PAGE 6 / 12

<table>
<thead>
<tr>
<th>ITEM #</th>
<th>DESCRIPTION</th>
<th>MODEL</th>
<th>QTY</th>
<th>UNIT PRICE (Euros)</th>
<th>LINE TOTAL (Euros)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Remote Intrusion Solution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>FinSpy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>FinSpy Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1</td>
<td>FinSpy Proxy License</td>
<td>TSPL</td>
<td>1</td>
<td>188,549.00</td>
<td>188,549.00</td>
</tr>
<tr>
<td></td>
<td>FinSpy Master License</td>
<td>FSML</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FinSpy Generation License</td>
<td>FSGL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>FinSpy Agent License (per client)</td>
<td>FSAGL</td>
<td>2</td>
<td>12,887.00</td>
<td></td>
</tr>
</tbody>
</table>

| SUBTOTAL | 280,787.00 |
| Freight   | 6,350.00   |
| TOTAL     | 287,137.00 |
FinFisher Global Proliferation

These are the results of scanning from DATE to DATE for known characteristics of FinFisher Command-and-Control servers.
1. Many servers may have been missed due to the scanning methodology.
2. Presence of a server does not necessarily indicate knowledge or complicity by the country to which it is connected.
3. *Servers identified during a previous scan.

YOU ONLY CLICK TWICE: FINFISHER ACROSS THE GLOBE

AUTHORS: MORGAN MARQUIS-BOIRE & BILL MARCZAK MAP: JOHN SCOTT TAITLON
Citizen Journalists Targeted
Citizen Journalists Targeted

"Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d'embrouilles…

http://freeme.eu5.org/scandale%20(2).doc"
“In the space of two hours on 20 December 2013, an attacker made three separate attempts to target two ESAT employees with sophisticated computer spyware”
ESAT - First Attempt

yalfalkenu Meches

An Article for ESAT.rar
File received. Show in folder

Please accept this article

Looking forward to hearing your comments
Remote Control System is totally invisible to the target. Our software bypasses protection systems such as antivirus, antisyware and personal firewalls.

Remote Control System gathers a variety of information from target devices.

- Encrypted voice
- Relationships
- Target location
- Web browsing
- Messaging
- Audio & Video Spy

Attack your target either remotely or locally using several installation vectors. Do that while the target is browsing the internet, opening a document file, receiving an SMS or crossing the borders with his laptop.
ESAT - Second Attempt

if it is a word file it should have extension like .doc or .docx
not .exe
the file that you end me has a file name like An Article for ESAT .exe
sent for me9

yalfalkenu Meches

An Article for Esat.doc
File received. Show in folder

got u. What you said makes sense
I got the doc file. Accept it

CVE-2012-0158 - Yay RTF!
New this week: CVE-2014-1761

It's 2014 and you can pwn a PC by opening a .RTF in Word, Outlook

Windows giant warns security flaw exploited in wild, but no patch available right now

By Jack Clark, 24 Mar 2014

Preparing for successful VDI implementation

Microsoft has warned its Word software is vulnerable to a newly discovered dangerous bug – which is being exploited right now in "limited, targeted attacks" in the wild. There is no patch available at this time.

The flaw is triggered by opening a maliciously crafted RTF document in the Microsoft Office word processor, or opening it via Outlook, and allows the attacker to execute arbitrary code on the machine.

http://www.theregister.co.uk/2014/03/24/microsoft_rtf_vuln/
Exploits today

- Only if they have to
- Old ones work
- The 0 days are out there...
- ... and they are for sale.
Backdoored Circumvention Tools - Simurgh

Welcome to the Simurgh Installation!

This setup program will install Simurgh on your computer. Click Cancel if you do not want to install this application. Click Next to continue the installation.

WARNING: This program is protected by international copyright law and treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent of the law.
Backdoored Circumvention Tools - FreeGate

![FreeGate 7.35 Professional Edition](image)

![Application Data](image)

---

```
[.ShadowTech_Rat.]
[exe.ShadowTech_R]
[\ta.ShadowTech_Ra|]
[\t.ISerializable.]
[\System.Runtime.Si]
[\erialization.MyS]
[\settings.ShadowTe]
[\ch_Rat.My.Applic|
```

---

Malware

Working copy of freegate
Backdoored Circumvention Tools - Tor
Ngoc Thu ran the largest political blog outside of Vietnam. Hacked in Jan 2013, personal information of website owner posted. Site shut down.


EFF bloggers targeted in December 2013.

Associated Press reporter targeted in December 2013.

This article appeared Jan 20th, 2014.
Phishing

The scariest lame threat
 Ensuring your information is safe online

June 1, 2011

The Internet has been an amazing force for good in the world—opening up communications, boosting economic growth and promoting free expression. But like all technologies, it can also be used for bad things. Today, despite the efforts of Internet companies and the security community, identity theft, fraud and the hijacking of people's email accounts are common problems online.
The Associated Press

Breaking: Two Explosions in the White House and Barack Obama is injured

10:07 AM - 23 Apr 13

The @AP Twitter account has been suspended after it was hacked. The tweet about an attack on the White House was false.

10:27 AM - 23 Apr 13
Reducing hijacking
Introducing Login Approvals

Facebook has always been committed to protecting your information, as well as giving you more control over your data. We want to further secure community, implement new security features like Facebook’s security management, everyone at Facebook experience.

Every time you sign in to Facebook, you’re prompted for your username and password. If you’re using Facebook Multi-Factor Authentication (MFA), you’ll also be asked to enter a code from your mobile device.

AWS Multi-Factor Authentication

AWS Multi-Factor Authentication (AWS MFA) provides an extra level of security that you can apply to your AWS environment. With AWS MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password (the first factor – what they know), as well as for an authentication code from their AWS MFA device (the second factor – what they have).

The Official Microsoft Blog

Microsoft Account Gets More Secure

Over the next couple days we will roll out a major upgrade to Microsoft account, including optional two-step verification to help keep your account more secure.

Getting started with login verification

Every day, a growing number of people log in to Twitter. Usually these login attempts come from the genuine account.
A CRYPTO NERD'S IMAGINATION:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
The Revolution

Will be televised on Youtube
Syrian Targeting of Citizen Media

Syrians on youtube

http://www.youtube.com/watch?v=PCg6FSLBmIw
http://www.youtube.com/watch?v=dJCIsU6QghI
http://www.youtube.com/watch?v=NHIR1ffBs_U

flag report>>> Violent or repulsive content>>>prompt terrorism
Microsoft tightens privacy policy after admitting to reading journalist's emails

After outrage from privacy campaigners, the tech firm will now seek legal advice before examining the contents of customers’ inboxes.

Alex Hern
Follow @alexhern Follow @guardiantech
theguardian.com, Friday 21 March 2014 06.34 EDT
Jump to comments (142)
Regional flavor
<table>
<thead>
<tr>
<th>RANK</th>
<th>NEWS SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>nytimes.com</td>
</tr>
<tr>
<td>2</td>
<td>indiatimes.com</td>
</tr>
<tr>
<td>3</td>
<td>wsj.com</td>
</tr>
<tr>
<td>4</td>
<td>usatoday.com</td>
</tr>
<tr>
<td>5</td>
<td>washingtonpost.com</td>
</tr>
<tr>
<td>6</td>
<td>latimes.com</td>
</tr>
<tr>
<td>7</td>
<td>examiner.com</td>
</tr>
<tr>
<td>8</td>
<td>smh.com.au</td>
</tr>
<tr>
<td>9</td>
<td>sfgate.com</td>
</tr>
<tr>
<td>10</td>
<td>chron.com</td>
</tr>
<tr>
<td>11</td>
<td>thehindu.com</td>
</tr>
<tr>
<td>12</td>
<td>nypost.com</td>
</tr>
<tr>
<td>13</td>
<td>hindustantimes.com</td>
</tr>
<tr>
<td>14</td>
<td>eenadu.net</td>
</tr>
<tr>
<td>15</td>
<td>chicagotribune.com</td>
</tr>
<tr>
<td>16</td>
<td>hollywoodreporter.com</td>
</tr>
<tr>
<td>17</td>
<td>indianexpress.com</td>
</tr>
<tr>
<td>18</td>
<td>theglobeandmail.com</td>
</tr>
<tr>
<td>19</td>
<td>theage.com.au</td>
</tr>
<tr>
<td>20</td>
<td>manoramonline.com</td>
</tr>
<tr>
<td>21</td>
<td>amarujala.com</td>
</tr>
<tr>
<td>22</td>
<td>washingtontimes.com</td>
</tr>
<tr>
<td>23</td>
<td>thestar.com</td>
</tr>
<tr>
<td>24</td>
<td>dnaindia.com</td>
</tr>
<tr>
<td>25</td>
<td>nj.com</td>
</tr>
</tbody>
</table>

*From Alexa Top 25 New as of 03/23/2014 by @ashk4n*
Hide yo sources, Hide yo docs

They be hacking everyone out here
How we fix this

- Journalists: Security integral to your job
- Security Industry: We can do better...
- Governments: well...