Tackling modern cyberthreats together is the only way forward

Romain Wartel, CERN
CHEP 2019, 4-8 November 2019, Adelaide, Australia
Welcome to the world of cybercrime

Alex Cazes (25 year old)  owner (3 years)

"Like Reddit, but for criminals"

190 000 registered members
Our community is a viable market for cybercriminals

And they are very aware of it
Emotet

• Email is the leading infection vector in our community (dedicated talk this morning)

• Current trend: content-aware phishing

source: kryptoslogic.com
Emotet at CERN

Real, legitimate email exchange with the targeted CERN employee

Emotet ☠
(exploits ongoing email threads)

Real, legitimate email exchange with the targeted CERN employee

(Shared with the permission of the targeted CERN employee)
Identity stealing & reselling

- Works on Windows XP/Vista/7/8/8.1/10 (all x86/x64)
  Windows Server 2003/R2, 2008/R2, 2012/R2 (all x86/x64)

- Bin size ~130kb (Uncompressed/raw balloon), ~85kb (compressed)

- Intuitive PHP Panel

- Bugfix, Updates and Support is free.

- Skype contact: [redacted]

Please confirm the Skype through PM here first because I got so many impersonators.
Identity stealing & reselling

• Identity management directly impacts our ability to collaborate, and to operate
  – Crucial aspect of our trust model (see AAI talk)
• There is a thriving market to sell academic & research identities

« I want to buy identities offering SSH access to academic, research or government-owned computing infrastructures. »
Credential theft: online markets

Dear users online store "AKAUNITY.ru", this site is specifically designed just for you! We are quite a unique site that not only sells the accounts, and buys them. In stock accounts have all the social networks on the ideal prices. If you can not find any accounts that you need, you can make an order for their registration in our online store.

Our accounts are benign. For convenience and product warranty with the purchase you have 20 minutes to check the accounts, so that you have verified their robot. Here you can find accounts for every taste: Facebook, Odnoklassniki, Vkontakte, etc.

Preparation of accounts is carried out instantly thanks to the automatic payment: Kiwi, Webmoney and Yandex.

Pleasant to use!
<table>
<thead>
<tr>
<th>Currency</th>
<th>Amount</th>
<th>Bank Type</th>
<th>Account Type</th>
<th>Account Details</th>
<th>Verification</th>
<th>Email</th>
<th>Status</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>US IA 52404</td>
<td>Verified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>USD</td>
<td>3.33</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>US NM 87121</td>
<td>Verified</td>
<td>N/A</td>
<td>01-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>MXN</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>MX N/A 2203624</td>
<td>Unverified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>USD</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>US IL 60532</td>
<td>Verified</td>
<td>N/A</td>
<td>06-04-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>EUR</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Premier</td>
<td>DE N/A 10785</td>
<td>Unverified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>USD</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Premier</td>
<td>US DE 19952</td>
<td>Verified</td>
<td>N/A</td>
<td>13-05-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>BRL</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>BR N/A 570</td>
<td>Unverified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>EUR</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Premier</td>
<td>DE N/A 10439</td>
<td>Verified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>USD</td>
<td>0.00</td>
<td>No bank accounts</td>
<td>Personal</td>
<td>US MI 48601</td>
<td>Verified</td>
<td>N/A</td>
<td>02-06-2017</td>
<td>N/A</td>
</tr>
<tr>
<td>USD</td>
<td>853.48</td>
<td>Family First Credit Card</td>
<td>Premier</td>
<td>US MO 63020</td>
<td>Verified</td>
<td>N/A</td>
<td>26-05-2017</td>
<td>18.15$</td>
</tr>
</tbody>
</table>

**Account:** uni.edu
## Credential theft: online markets

| Platform          | Processor        | RAM (GB) | CPU Speed (GHz) | Download Speed (MB/s) | Upload Speed (MB/s) | Country       | State       | City       | Zip        | Price ($) |
|-------------------|------------------|----------|-----------------|-----------------------|---------------------|---------------|-------------|------------|------------|-----------|-----------|
| Windows 7 (Spanish) | Intel Pentium CPU G2... | 1.89 GB  | 0.46 MB/s | 1.05 MB/s | Country: Argentina | State: Santa Fe | City: Villas Canas | Zip: 2617 | 29-05-2017 | 3,389     | 5,265     |
| Windows 7 (Portuguese) | Intel Core(TM) i7-3770 ... | 3.39 GB  | 1.32 MB/s | 3.38 MB/s | Country: Brazil | State: Bahia | City: Canoas | Zip: 43306 | 29-05-2017 | 3,389     | 5,875     |
| Windows 7 (Spanish) | Intel Core(TM) i5-4460C... | 15.88 GB | 10.14 MB/s | N/A       | Country: Colombia | State: N/A | City: N/A | Zip: N/A | 29-05-2017 | 3,389     | 5,725     |
| Windows Server 2008 (Arabic) | Intel Core(TM) 2 Duo CP... | 3.94 GB  | 0.44 MB/s | 3.41 MB/s | Country: Egypt | State: N/A | City: N/A | Zip: N/A | 29-03-2017 | 3,389     | 4,355     |
| Windows 7 (Portuguese) | Intel Core(TM) i3-6300 ... | 3.33 GB  | 1.41 MB/s | 4.6 MB/s | Country: Brazil | State: Rio de Janeiro | City: N/A | Zip: N/A | 29-05-2017 | 3,389     | 6,445     |
| Windows 7 (Spanish) | Intel Core(TM) i7-6700 ... | 31.88 GB | 3.62 MB/s | 5.45 MB/s | Country: Colombia | State: Valle del Cauca | City: Cali | Zip: N/A | 29-05-2017 | 3,389     | 6,45      |
Credential theft: online markets

<table>
<thead>
<tr>
<th>OS / Lang</th>
<th>CPU / Core / Bits OS</th>
<th>Ram</th>
<th>AV</th>
<th>Browse</th>
<th>Speed UP/DL</th>
<th>Root</th>
<th>NAT</th>
<th>Poker</th>
<th>Geo Location</th>
<th>Checked</th>
<th>Port</th>
<th>Not Used</th>
<th>Seller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>Common KVM processor</td>
<td>3.20 GB</td>
<td><img src="antivirus.png" alt="Antivirus" /></td>
<td><img src="browser.png" alt="Browser" /></td>
<td>UP: 2.85 MiB/s DL: 28.01 MiB/s</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Country: Brazil State: Paraíba City: Queimadas Zip: N/A</td>
<td>15-05-2017</td>
<td>3389</td>
<td></td>
<td>sereb</td>
</tr>
<tr>
<td>(Portuguese)</td>
<td>CPU Core: 4 Bits OS: 32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7</td>
<td>Intel(R) Xeon(R) CPU E5-2620v4</td>
<td>4.00 GB</td>
<td><img src="antivirus.png" alt="Antivirus" /></td>
<td><img src="browser.png" alt="Browser" /></td>
<td>UP: 9.21 MiB/s DL: 14.1 MiB/s</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>Country: Brazil State: N/A City: N/A Zip: N/A</td>
<td>15-05-2017</td>
<td>3389</td>
<td></td>
<td>sereb</td>
</tr>
<tr>
<td>(Portuguese)</td>
<td>CPU Core: 2 Bits OS: 64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Our community is also targeted by Nation State actors —

Collateral victims of global digital warfare
# APT Operations and Groups

https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4Q_Son4Gx0YOIzIcBWMsdvePFX68EKEU/edit?#gid=1864660085

<table>
<thead>
<tr>
<th>Unknown / Unmapped Actors</th>
<th>Toolset / Malware</th>
<th>Targets</th>
<th>Comment</th>
<th>Link 1</th>
<th>Link 2</th>
<th>Link 3</th>
<th>Link 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unknown / Unk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Crouching Yeti</td>
<td>Toolset</td>
<td>Targets</td>
<td>Comment</td>
<td>Link 1</td>
<td>Link 2</td>
<td>Link 3</td>
</tr>
<tr>
<td>4</td>
<td>New Romanic Cyber</td>
<td>Whois</td>
<td>Wiper</td>
<td>Links to Energetic Bear</td>
<td><a href="https://securelist.co">https://securelist.co</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The Whois Hacking</td>
<td></td>
<td></td>
<td><a href="http://www.mcafee">http://www.mcafee</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ItaDuke</td>
<td></td>
<td></td>
<td><a href="http://www.mcafee">http://www.mcafee</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Roaming Tiger</td>
<td>Russian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Blue Termite</td>
<td></td>
<td></td>
<td>This threat actor is believed to have been responsible for the Japan Pension Service Incident. It is also known as Emdivi and Cloudy Omega.</td>
<td><a href="https://kaspersky.ru">https://kaspersky.ru</a></td>
<td><a href="https://web.archive.org">https://web.archive.org</a></td>
<td><a href="http://www.symantec.com">http://www.symantec.com</a></td>
</tr>
</tbody>
</table>
Current market prices
How the acquired security research is used by ZERODIUM?

Who are ZERODIUM's customers?

ZERODIUM customers are mainly government organizations in need of specific and tailored cybersecurity capabilities and/or protective solutions to defend against zero-day attacks.

Access to ZERODIUM solutions and capabilities is highly restricted and is only available to a very limited number of organizations. ZERODIUM does not have any sales partner or reseller, our solutions are only available through our direct channel.

Is ZERODIUM hiring security researchers and/or reverse engineers?
Verizon’s 2019 data breach report covering 86 countries and 41,686 intrusions:

«23% of bad actors are identified as nation-state or state affiliated»
APT Operations and Groups

APT40

Suspected attribution: China

Target sectors: APT40 is a Chinese cyber espionage group that typically targets countries strategically important to the Belt and Road Initiative. Although the group targets global organizations — especially those with a focus on engineering and defense — it also historically conducted campaigns against regional entities in areas such as Southeast Asia. Since at least January 2013, the group has conducted campaigns against a range of verticals including maritime targets, defense, aviation, chemicals, research/education, government, and technology organizations.

Overview: FireEye Intelligence believes that APT40’s operations are a cyber counterpart to China’s efforts to modernize its naval capabilities; this is also manifested in targeting wide-scale research projects at universities and obtaining designs for marine equipment and vehicles. The group’s operations tend to target government-sponsored projects and take large amounts of information specific to such projects, including proposals, meetings, financial data, shipping information, plans and drawings, and raw data.

Associated malware: APT40 has been observed using at least 51 different code families. Of these, 37 are non-public. At least seven of these non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are shared with other suspected China-nexus operators.

Attack vectors: APT40 typically poses as a prominent individual who is probably of interest to a target to send spear-phishing emails. This includes pretending to be a journalist, an individual from a trade publication, or someone from a relevant

Additional resources

Blog - APT40: Examining a China-Nexus Espionage Actor
EternalBlue — Story of an NSA 0-Day

The Shadow Brokers

Public leak 2017

2016

APT3

First known attack

March 2016

NotPetya

WannaCry
300,000 infections
EternalBlue — Story of an NSA 0-Day

- Very expensive « 0-day » vulnerabilities are used against our community

The Shadow Brokers

Public leak 2017

Educational institution in Belgium

First known attack

March 2016

WannaCry

300,000 infections

NotPetya

Educational institution in Belgium

2016

APT3

BUCKEYE

The Shadow Brokers

2016
APT34: Oilrig

- Fake LinkedIn profiles and invites to a conference
- Example domains:
  - oxford-symposia[.]com or oxford-symposium[.]com

- Downloads signed malware
APT34: Oilrig

University Of Oxford Jobs Symposium Pre-Registration Tool

In this symposium:
- New scientific articles.
- Introduction of new job opportunities.
- Introduction to large commercial and industrial companies.
- You can use your articles in their field for us and we will record them in your name.
- We have over 20,000 articles, experiences and job opportunities will be presented to you.
- You can participate in person or virtual meetings or classes.
- We can arrange for you meetings with human resources departments of companies that are at the symposium.
- We can help you in your career to be more efficient and more professional.

University of Oxford jobs symposium - February 6, 2017 - February 23, 2017
An Iranian hacking group was itself hacked by a Russian group to spy on multiple countries, UK and US intelligence agencies have revealed.

The Iranian group - codenamed OilRig - had its operations compromised by a Russian-based group known as Turla.

The Russians piggybacked on the Iranian group to target other victims.

A National Cyber Security Centre (NCSC) investigation, begun in 2017 into an attack on a UK academic institution, uncovered the double-dealing.

Crowded space

The NCSC discovered that the attack on the institution had been carried out by the Russian Turla group, which it realised was scanning for capabilities and tools used by Iran-based OilRig.

In an investigation that lasted months, it became clear the Russian group had targeted the Iranian-based group and then used its tools and access to collect data and compromise further systems.

Attacks were discovered against more than 35 countries with the majority of the victims being in the Middle East. At least 20 were successfully compromised.
Silent Librarian Phishing Campaign

Posted on April 8, 2019, modified on April 10, 2019 by

The Office of Information Security ("OIS") has been made aware of a phishing campaign dubbed "Silent Librarian" that is targeting the NYU community. This phishing campaign is designed to steal login credentials, and has been targeting universities, companies and government agencies around the world. Silent Librarian has targeted more than 300 universities in 22 countries, and the cost to universities alone is estimated to be around 3.4 billion.

The following is an example of a Silent Librarian phishing message.

Dear Member,

This message is to inform you that your access to the library will soon expire. You will have to login to your account to continue to have access to this service. You can reactivate it by logging in through the following URL. A successful login will activate your account and you will be redirected to your page.

http://shibboleth.nyu.nibb.ni/idp/profile/SAML2/POST/SSO.execution

If you are not able to login, please contact XXXXXXXX@nym.edu for immediate assistance.

Sincerely,

[Signature]

New York University
50 West Fourth Street
New York, NY 10003

Attacks continue today...
Cybercriminals: opportunistic
Cybercriminals: targeted

Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"
Nation-state attack

Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"
Only one strategy:
Leveraging our community to secure together its individual members
—
Both for threat intelligence and incident response
Trust and threat intelligence

• As a global community we have strong assets
  – Often share tools, services and users/victims (similar vulnerabilities and entry points)

• Responding to threats as a community for daily security operations:
  – First member observing an attack shares indicators with others
  – Mutualize expertise and knowledge to provide a community-based response

• Best way of fighting sophisticated adversaries at acceptable costs
A community response

1. Trust and collaboration
2. Threat intelligence sharing
3. Security Operations Centre
4. Joint security operations and incident response

IOC = Indicator of compromise
A community response

IOC = Indicator of compromise

(See dedicated talk)
A community response

Trust Framework
Trust group(s)
IOCs sharing platform

Gov. CERT
IOC = Indicator of compromise

Vendor

Local community

(See dedicated talk)
• Consistent experience within our community in the last 5 years:
  – Attacks are increasingly global and more sophisticated
  – Few, highly skilled individuals provide significant technical expertise to victims
  – Recurring lack of:
    • Technical: incident response procedures, traceability information
    • Human: Collaboration, security contact points, trust and expertise

• Collaboration with law enforcement and the private sector essential

• Golden Triangle:
  – Law Enforcement: Can arrest criminals and seize assets
  – Private sector: Have time and expertise
  – Our sector: Can reach out to victims, access evidence and trusted security contacts
• Ad-hoc team of incident response coordinators
  – Manage and centralise the information flow and evidence (may be 1000+ victims)
  – Disseminate the right details to all potential victims (direct or via e-infrastructure)
  – Focus the investigation on identified goals (key leads)
  – Mutualise the collective expertise of involved experts (IOCs, scanner, decryptors)
  – Interface directly with third parties (law enforcement)
Central coordination: who is this?

- Everyone’s business but nobody’s job
- Always need ad-hoc teams to manage global severe intrusions
- Usually composed of energised individuals from our community (and wider)
  “If you are interested to defend against this attack and have some time to dedicate to this, welcome onboard!”

Example: Operation Windingo
Global incident response workflow model

- Each communication link is either:
  - Pre-established trust framework (faster at large scale)
  - Known personal contact or trust built ad-hoc (slower)
- Different collaboration tools and changing/converging is extremely difficult
Global incident response workflow model

- Scope is all relative
- Multiple levels of coordination, depending on severity, scale & location:
  - « Local » coordination for a project, community or e-infrastructure
  - Global coordination generally involves private sector and/or law enforcement
Impact of federated identities on incident response

- Federations must provide incident response capabilities similar to einfrastructures.
- Grid incident, academic security incident, federated security incident…

Does classification matter? Where is the boundary?

- We are bound to have a collection of interconnected trust groups.
Summary of lessons learnt

• We are a viable market for cybercriminals and are targeted by Nation States actors
  – Connecting and defending as a community is the only way forward
• It is not enough to have prearranged channels and procedures
  – Trust frameworks and established incident response procedures essential
  – Ad-hoc communication & organisation always necessary
• Deploying Security Operation Centres (e.g. MISP + Bro/Zeek) is essential
• Global incident response is difficult
  – Coordination is nobody’s job
• Our community has great expertise and skills available
  – Analysis & forensics, tools, etc.
• Investing in threats affecting others/the community offers priceless benefits
  – Precious allies, trusted security contacts, advanced security tools, great threat intelligence
Thank you

Discussion