VENOM: DISCOVERY OF A NEW MALWARE

- 14\textsuperscript{th} of Dec 2016: a site in central Europe reports a root compromise

- Yesterday (13\textsuperscript{th} of Dec), during standard operations activities we revealed a malicious process running on one of our DPM servers <SNIP>. The process seems to provide a backdoor access to the system. It was run under the root user and automatically started upon system boot.

- A more detailed investigation is ongoing right now. We still don't know how the malware got to the box or other details about the intrusion.

- The process in question was running off a program placed in /var/lib/mkinitramfs, which is a dynamically built ELF executable
VENOM: MALWARE ANALYSIS

- Linux VENOM rootkit, never seen before
- Contributions from multiple experts (US, Europe, Asia)
- The malware has two components:
  - Userland encrypted backdoor with remote code execution and proxy functionalities
  - Kernel part featuring additional port-knocking for the backdoor, requiring 3 specific TCP packets:
    TCP Source Port + Sequence Number == 1221
- Mysterious P2P traffic on TCP/9090 between compromised hosts
  - Used for copying source + binaries files between victims?
VENOM: MALWARE ANALYSIS

- Actors behind have excellent opsec:
  - Binaries are compiled on the victim’s machine in /dev/shm
  - Paths, including runtime, are changed to always resemble a legitimate or expected Linux system component
    - /var/lib/mkinitramfs, /etc/X11/applnk/.window, /usr/share/man/man5/printers_cupsd.conf.5.gz, crond, ...
  - Local log files are erased and filesystem timestamps are manipulated
  - Persistence across system reboot is relying on a modification of the system init scripts (/etc/rc.d/init.d/functions)
INFECTION VECTOR:

\[ \text{pnarolkr} = \"e\" + \"^\" \]
\[ \text{mtfmzvef} = \"M\" \]
\[ \text{yzdlnepo} = \text{pnarolkr} + \text{mtfmzvef} \]
\[ \text{xrnzczjm} = \"a\" \]
\[ \text{fkiphfyl} = \"I\" + \"l\" \]
\[ \text{swcaxaca} = \text{yzdlnepo} + \text{xrnzczjm} + \text{fkiphfyl} \]
EMAIL AS AN INFECTION VECTOR

- Easiest way into an organization & most popular infection vector
- Generic platforms, more and more dynamic payloads
  - From Switzerland, on a Windows 7 machine? Get a banking trojan!
  - From US, on a Windows 10 machine? Get some ransomware!
- Two main techniques
  - Malicious attachements (Microsoft Office, JS, PDF, etc.)
  - Malicious URL (random TLDs, but also AWS, Google Drive, Dropbox, compromised Wordpress, etc.)
- Difficult to detect and block
- Oh, and users will make significant efforts to click!
MAILING CAMPAIGN AT CERN FOR AWARENESS RAISING

- Email messages designed by students at the University of Rotterdam
  - No inside knowledge of CERN
- Click rate in 2016: 16.54%*
- Click rate in 2017: 18.7%
- Percentage of the people that clicked in 2016 and again in 2017: 24.5%
A total of 938 people out of 19,880 recipients contacted us

- The majority reported it as phishing and asked to have it blocked
- Some were asking if this is one of our campaigns
- And some were asking for what to do after having clicked
ANYONE BEEN TO CHINA RECENTLY?

Is the sender familiar to you?

Does the sender’s name correspond with the shown e-mail-address?

Is the message signed ( 🐦 )?

Is the message addressed to you?

Is the message correctly phrased, without blunt typos, in a language you are able to comprehend?

Does the message concern you? Is it one of your businesses?

Hover your mouse pointer on top. Does the text correspond with the link?

Does the link look reasonable, is not too complex or unreadable?

If you have answered any one of those questions with “NO” be vigilant and careful! Delete that message or check with us at Computer.Security@cern.ch when in doubt.
SOME MESSAGES ARE MORE EFFECTIVE THAN OTHERS

Two of the 5 messages used accounted for half of the number of clicks.
MOST PEOPLE WERE CLICKING FROM OUTSIDE CERN

Blocking malware and phishing domains at the DNS level not 100% efficient
MORE THAN HALF CLICK WITHIN ONE HOUR FROM EMAIL BEING SENT

Ideally blocking should happen before emails start arriving
NOT DELIVERING EMAILS TO USERS

- Email is business critical - false positive not well accepted
- Making an accurate and fast determination of incoming email is crucial
The devil is in the details

- Cloud provider rules?
  - Detects low-end malware only

- Org. rules in the cloud
  - Signature based only, few options

- Org. rules on premise
  - Sandboxing behavior analysis < 2 min
  - 2 min to convince malware that this is not a sandbox

- User email client
  - Local rules
  - AV
  - “Hardening”
  - Very late + Large surface

- Network rules (DNS, IP, domains)
  - Signature based only, few options

MALICIOUS PAYLOAD
Randomised:
- From field, subject, email body, attachment (each has a different hash and filename)
- Multiple payload URI
  - Dozens of unique URIs, with randomised query strings
- Frequently changes:
  - Obfuscation techniques, file extensions (.doc, .docx, .docm, .pptm, .wsf, etc.), X-Mailer field, anti-analysis techniques (check of process count, process names, count of recent files, etc)
- Actual C2s, or payment domains typically more stable
## The 10 Most Abused Top Level Domains

<table>
<thead>
<tr>
<th>Rank</th>
<th>TLD</th>
<th>Badness Index</th>
<th>Badness Index</th>
<th>Domains seen: 56,325</th>
<th>Bad domains: 51,335 (91.1%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.science</td>
<td>9.23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>.men</td>
<td>7.19</td>
<td></td>
<td>Domains seen: 67,879</td>
<td>Bad domains: 45,522 (67.1%)</td>
</tr>
<tr>
<td>3</td>
<td>.webcam</td>
<td>6.90</td>
<td></td>
<td>Domains seen: 17,673</td>
<td>Bad domains: 12,881 (72.9%)</td>
</tr>
<tr>
<td>4</td>
<td>.stream</td>
<td>6.62</td>
<td></td>
<td>Domains seen: 8,874</td>
<td>Bad domains: 6,669 (75.2%)</td>
</tr>
<tr>
<td>5</td>
<td>.click</td>
<td>6.31</td>
<td></td>
<td>Domains seen: 12,944</td>
<td>Bad domains: 8,375 (69.3%)</td>
</tr>
<tr>
<td>6</td>
<td>.top</td>
<td>6.11</td>
<td></td>
<td>Domains seen: 253,572</td>
<td>Bad domains: 131,475 (51.8%)</td>
</tr>
<tr>
<td>7</td>
<td>.study</td>
<td>5.39</td>
<td></td>
<td>Domains seen: 586</td>
<td>Bad domains: 507 (86.5%)</td>
</tr>
<tr>
<td>8</td>
<td>.gdn</td>
<td>5.23</td>
<td></td>
<td>Domains seen: 22,957</td>
<td>Bad domains: 12,716 (55.4%)</td>
</tr>
<tr>
<td>9</td>
<td>.cricket</td>
<td>5.13</td>
<td></td>
<td>Domains seen: 3,485</td>
<td>Bad domains: 2,309 (66.3%)</td>
</tr>
<tr>
<td>10</td>
<td>.link</td>
<td>5.05</td>
<td></td>
<td>Domains seen: 14,599</td>
<td>Bad domains: 8,186 (56.1%)</td>
</tr>
</tbody>
</table>

- Have you seen any legit use for most of these TLDs?
- How about blocking access to them at the DNS / proxy level?

Source: [https://www.spamhaus.org/statistics/tlds/](https://www.spamhaus.org/statistics/tlds/)
- Threat intelligence plays a key role in daily operations
- More than 160,000 IoCs available in the WLCG MISP
  - Get in touch with me if you would like to get access
CLOSING REMARKS

‣ How to make best use of the threat intel available in the community?
‣ How can we improve collaboration between campus security and site security?
‣ What can we do to help?