Surviving and operating services despite highly skilled and well-funded organised crime groups

Romain Wartel, CERN
CHEP 2015, Okinawa
• 30,000+ unique servers compromised in the last two years
  – kernel.org, Linux Foundation, CPanel, many universities and research lab, public and private sector organisations

• A full ecosystem of advanced malware
  – Ebury: SSH backdoor. Controls servers + steals credentials
    (signed RPM installed “in the past”. Infests libkeyutils.so)
  – LinuxCdorked: stealth, file-less, multi-platform HTTP backdoor
  – Perl/Calfbot: manages the payload, 35 million spams/day
  – Linux/Onimiki: supporting Linux DNS malware
  – Win32/Boaxxe.G: Click fraud malware
  – Win32/Glupteba.M: Generic proxy/downloader malware

• Not just software: large-scale malicious infrastructure
  – Fully distributed, complex infrastructure, using multi-tiered proxies, lots of obfuscation and encryption

• International gang, highly profitable activity - still ongoing
What are bad actors up to?

• No major evolution of the threat landscape
  – Same infection techniques, same rootkits
• No major evolution of the Linux & Windows malware
  – But most large attacks now target both platforms!
• Web (and Flash in particular) play prevalent role
• Significant uptake of Android malware
• iOS malware still very rare
  – But growing evidence of effective government-sponsored attacks
• Strong consolidation of the underground market/economy
  – Severe competition between a handful of exploit kits (EK)
  – Angler, Magnitude, Sweet Orange, Fiesta, RedKit, Nuclear, etc.
  – Huge progress on time-to-market for exploits
    • Only hours/days before vulnerabilities available in EK
    • CVE-2015-0311 discovered as a Flash “0-day” in Angler EK
Malware-as-a-service
Malware-as-a-service

RIG Customers

Malvertisement
Purchased traffic
Compromised website

Victim

1. Initial request
2. API to get updated Proxy URL
3. Iframe pointing to the Proxy server
4. Get relevant exploits and payload
5. Get the payload configured by the customer

Proxy Server

Main Admin Server

VDS Server
(exploits stored here)

Source: Trustwave
Malware-as-a-service

Statistics
Total hits 9091
Flow 701: 9091

Attack type (top 10)

<table>
<thead>
<tr>
<th>Name</th>
<th>Exploits</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>676</td>
<td>(50.6%)</td>
</tr>
<tr>
<td>ie10</td>
<td>452</td>
<td>(33.8%)</td>
</tr>
<tr>
<td>msie</td>
<td>209</td>
<td>(15.6%)</td>
</tr>
</tbody>
</table>

Countries (top 10)

<table>
<thead>
<tr>
<th>Name</th>
<th>Hits</th>
<th>Exploits</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE</td>
<td>1612</td>
<td>120 (7.4%)</td>
</tr>
<tr>
<td>IT</td>
<td>1238</td>
<td>193 (15.8%)</td>
</tr>
<tr>
<td>ES</td>
<td>1088</td>
<td>100 (13.7%)</td>
</tr>
<tr>
<td>US</td>
<td>721</td>
<td>80 (11.1%)</td>
</tr>
</tbody>
</table>

Source: Trustwave
Malware-as-a-service

Source: Trustwave

Each customer can have 2 flows and 2 different EXE payloads
Каждый аккаунт имеет 2 потока и может грузить 2 разных exe

API with automatic exploit delivery
API for automatic landing page URL

List of exploits
- Java: CVE-2012-0507
- Java: CVE-2013-2465
- IE7-8-9: CVE-2013-2551
- Flash: CVE-2015-0313
- Windows: CVE-2014-6332

Average exploitation rate
Средний пробив 10-15%

Prices:
- 24 hours - $30
- One Week - $150
- One Month - $500

Source: Trustwave
Getting the victims to click

- **Web:** Gigantic attack surface
  - Vulnerabilities (browser, PDF, Flash, etc.)
  - Malvertisement
  - Compromised (legitimate) websites
  - Social network applications or plugins
  - Malicious browser plugins, extensions

- **Email:** leading source of compromise
  - 90%+ of breaches caused by spear phishing
  - Extremely effective:
    - 10 emails = 1 click guaranteed
    - Targeted phishing: ~70% success rate
Learn & adapt

• Defend your organisation or (Linux) data center
  – Must start defending Windows/Web/mobile realms too
  – Ultimately, must defend people

• International collaboration is our main asset
  – Main intrusion detection system at CERN in the last 5 years

• International community: sharing and trusting
  – Strong knowledge on attack methods and tools
  – Report about actual compromises or data leaks in our community
  – Invaluable intelligence
  – Engage & participate!

• Work on connections with industry and law enforcement
  – Attackers arrested on a regular basis for attacking HEP organisations
Learn & adapt

• Protect your people:
  – Raise awareness
  – Organise training events (tools, methods)
  – Write and advertise clear policies
  – Do not overlook personal use and devices

• Protect your organisation
  – Understand your adversaries
  – Invest resources to have sufficient in-house capabilities
  – Contribute to global efforts against cybercrime (botnet takedown…)
  – Build your network of contacts in the security community
  – Invest in threat intelligence and technical means to use it
  – Treat security incidents as part of normal operations
Raising the bar

Common sense and sysadmin good practice

Government security agency

Targeted criminal organisation

Untargeted criminal organisation

Script kiddy

Adversary sophistication

“Unfavorable battleground” - Outcome unlikely positive
Focus on protecting your people as best as possible
Engage with community and dedicated experts
Hire external (forensics, intel) consulting if needed
Threat intelligence, international collaboration
Advanced monitoring + traceability (SoC)
Common sense and sysadmin good practice
Getting “80%” protected

• Mail, or instant messaging
  – Absolutely never click on links from emails
  – Preferably go directly to the homepage of the website
  – If not easily possible, copy/paste and carefully verify the link
  – Malware comes via links or attachments (PDF, DOC, PPT)
  – Unexpected email? Unknown sender? Unusual language? Factual mistakes and typos? Unusual request or practices?

• Web: Stop. Think. Click.
  – Prefer Chrome, or at least Firefox, over Internet Explorer
  – Use a different Web browser for personal & professional use
  – Never click on popup windows or on “update” links for Flash or other plugins
  – If possible, disable or at least configure “click-to-play” for Flash
  – Do not install plugins or extensions. Absolutely never install drivers, video codecs, video players, add-ons bars
• Computers
  – Keep up-to-date with security patches. Enable automatic patching
  – Run a good anti-virus
  – Install or update from trusted sources only (your lab, Apple App Store, directly from the official vendor website). Never CNET/download.com, etc.

• Phones
  – Android is the primary target for malware
  – Many Android phones very difficult to patch and very quickly unsupported
  – Think before installing (check permissions required, user reviews, number of downloads, etc.)
Conclusions

- Criminal groups equally target Linux and other platforms
  - Target victims
  - Operate their services

- Expect large-scale and sophisticated attacks

- Protecting services is no longer sufficient
  - Must defend people
  - Across all their devices, both professional and personal
  - Improve their online hygiene

- Web and mobile platforms are primary targets

- International collaboration is the a key aspect of defence