Building community playbooks for malware eradication
Christian Seifert
Microsoft Malware Protection Center
Security@Microsoft

**Trustworthy Computing (TwC)**
- Programs supporting security outreach and engagement
- Microsoft Active Protections Program (MAPP), Government Security Program (GSP) (was SCP)

**Microsoft Security Response Center (MSRC)**
- Vulnerabilities in Microsoft software and services (secure@microsoft.com)

**Digital Crimes Unit (DCU)**
- Botnet takedowns
- Engage law enforcement

**Microsoft Malware Protection Center (MMPC)**
- Malicious Software Removal Tool (MSRT – monthly scan & remove)
- RTP - Security Essentials, System Center Endpoint, Windows Defender, Threat Intel
MMPC by the numbers

Research labs in Redmond, Vancouver, Munich, Melbourne
Engineering labs in Redmond and Israel

PROTECTION POINTS

- Windows 8+ Defender 110M
- System Center EP 11M
- Microsoft Security Essentials 109M
- Malicious Software Removal Tool 1.2B
- Outlook.com O365
- Skype
- Azure

DAILY
- 700K samples
- 400M telemetry
- 12 sig releases
  - 12x/yr engine
  - 3x/yr Client updates

RESULTS
- 6.5% encounters
- 3% infected
  - (1 Malware; 2 UwS)
- 100M unique files
- 80% running AV
What is CME?

A collaboration program sponsored by the Microsoft Malware Protection Center; created in early 2014

Facilitates campaigns targeting specific, pervasive malware families

Members of CME use the framework & Microsoft’s tools/data/research/capabilities to lead or take part in campaigns against malware families
Antimalware and security ecosystem
- identify, block, sinkhole

Digital Crimes Unit
- Law enforcement
  - seize, prosecute

CERTs, ISPs
- set policies, takedown

Large-scale public services
- Cloud platform providers
  - identify, block

Ad networks
- Banks, finance, commerce
  - starve

OEMs
- Vendors
  - shun

Coordinated Malware Eradication
Members of CME use the framework to take part in or lead campaigns against malware families.

**CME members**
- Decide and organize campaigns
- Leverage and contribute to campaign documentation and best practices, collaboration tools, and exchange telemetry and forensic data to vet and run campaigns.
- Use the rolodex and the MS CME support team for additional help as needed

**Member directory**

**Process & best practices**

**Collaboration tools**

**Telemetry and forensic data repository**

**Campaign managers**
- Check in with CME support team for guidance
- Provide reports on campaign health

**MS CME support team**
- Coaches CME members to launch campaigns
- Helps campaigns leverage tools
- Drives program updates/new tools
- Reports campaign status to Microsoft leadership
Joining VIA (and CME)

The Virus Information Alliance (VIA) is an antimalware collaboration program for security software providers, security service providers, antimalware testing organizations, and other organizations involved in fighting cybercrime.

Members of the VIA program collaborate by exchanging technical information on malicious software with Microsoft, with the goal of improving protection for Microsoft customers.

http://aka.ms/mmpcpartner

Eligibility requirements posted on website

Membership application form available online at http://aka.ms/viaapply
Completed Campaigns

- Ramnit
- SMN
- Hesperbot
- Lecpetex
- Simda
Operation summary - Simda
Simda

- Detected since 2009
- Primarily distributed by exploit kits (Blackhole, Styx, Magnitude, Fiesta)
- Behaviors:
  - Internet traffic manipulation – HOSTS File
  - Distribute Other Malware – Miuref / Claretore / Haglacod
  - Anti-emulation
  - Older behaviors:
    - Password stealer
    - Banking trojan
    - Backdoor
- Estimated Reach: 770K last six months
Simda campaign overview

**Targeting info**
- PR Communications
- Run Sinkhole

**INTERPOL (FBI, NCA, Dutch High Tech Crimes Unit)**
- Attribution
- Coordinate C&C IP addresses, physical server seizures
- Law Enforcement communications and logistics

**Trend Micro**
- Execute and Analyze Simda Samples
- Long Term Analysis
- AV Cleaning Solution

**Kaspersky**
- Execute and Analyze Simda Samples
- Long Term Analysis
- AV Cleaning Solution

**CDI**
- Execute and Analyze Simda Samples
- Long Term Analysis

**Microsoft**
- Execute and Analyze Simda Samples
- Long Term Analysis
- AV Cleaning Solution
# Simda.AT Takedown: IP’s Status

<table>
<thead>
<tr>
<th>Country</th>
<th>Check In C2’s:</th>
<th>Module C2’s:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>United States</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- **Total IP’s Taken Down:** 16
- **Total ISP’s:** 9
- **Total Countries:** 5

New Samples: 1 – Truncated Copy of an Old Sample

[MMPC Blog](https://www.mmptactical.com/blog/post/simda-at-takedown-ip-s-status)
Microsoft, Kaspersky Take Down Fast-Spreading Simda Botnet

By Robert Lemos | Posted 2015-04-13

Interpol and European authorities take down a second botnet, cooperating this time with Microsoft, Kaspersky Lab and Trend Micro.

International law enforcement authorities at Interpol teamed up with Microsoft, the Cyber Defense Institute in Japan, and security firms Kaspersky Lab and Trend Micro to take down a second major botnet last week, in a coordinated effort to disrupt the criminal operation, the Interpol Global Complex for Innovation (IGCI) said in a statement on April 13.

The botnet, known as Simda.AT, has infected more than 770,000 systems in the past six months, attempting to redirect Internet traffic and download additional malware to compromised computers. Microsoft's Digital Crime Unit (DCU) alerted law enforcement to the botnet following a dramatic increase in activity, IGCI stated. The groups detected approximately 90,000 newly infected systems in the United States in the first two months of this year, according the IGCI.

The botnet's operators would steal information from compromised systems, re-route network traffic, and use their access to install other malware and software, Jon Clay, senior manager for global threat communications for Trend Micro, told eWEEK.

"With this botnet, their intention was to infect as many people as possible," he said. "And once they infected them, they could do pretty much anything they wanted to with these victims, whether it was steal financial information, use their systems to launch denial-of-service attacks or spam, or sell (access to) their computers off to other criminals."

We believe the bot is dismantled...

No new Simda.AT files have been observed. Infected computers still need cleaning for the host file.

<table>
<thead>
<tr>
<th>Families</th>
<th>Encounters</th>
<th>Actives</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>simda</td>
<td>78,359</td>
<td>57.0%</td>
<td>47.1%</td>
</tr>
</tbody>
</table>

Impact Per Day (Encounters)
Operation summary - Ramnit
Ramnit

- Detected since 2011
- Distribution Methods:
  - Viral spread in HTML and PE
  - Infected USB
  - Email attachments / SPAM / URL
  - Social networks
  - Exploits
- Modules / behaviors:
  - Banking credential stealer
  - FTP application credential stealer
  - Hook and spy / web inject
  - Cookie stealer
  - Anti-AV / tampering
  - VNC backdoor
  - Drive Scan
- Estimated reach: 3.2 million
Ramnit campaign overview

**Microsoft**
- Seize 7, register 289 domains
- Coordinate existing sinkholes
- Operate DNS, sinkhole traffic, reporting

**EC3-European Computer Crime Center**
- Physical server criminal seizure
- Lead attribution work, assist Europol on forensic analysis
- Coordinate PR communications

**Symantec**
- Technical review, telemetry.
- Industry outreach
- Technical legal declaration.
- Coordinate PR communications

**FS-ISAC**
- Co-plaintiff
- Coordinate communications with financial sector.
- Coordinate PR communications
217.23.11.117
95.141.36.218

Current C2 Server=bot registration, configuration, and modules.

95.141.36.218
93.190.138.126

Backup C2 server

148.251.35.151

Web inject server

148.251.35.151

Web inject server

5.9.224.198

EXPIRED 14 Feb 2015

Online 15 Feb 2015

Blue=Current IP
Red=Old IP
Europol Takes Down RAMNIT Botnet that Infected 3.2 Million Computers

**RAMNIT SHUT-DOWN IN AN OPERATION**

In a [statement](#) on Tuesday, Europol revealed that the successful take-down of Ramnit botnet involved the help of Microsoft, Symantec and AnubisNetworks. The groups shut down the botnet's command and control infrastructure and redirected traffic from a total of 300 domain addresses used by Ramnit criminal operators.

“This successful operation shows the importance of international law enforcement working together with private industry in the fight against the global threat of cybercrime,” said Wil van Gemert, Europol’s deputy director of operations. “We will continue our efforts in taking down botnets and disrupting the core infrastructures used by criminals to conduct a variety of cybercrimes.”

**NASTY FEATURES OF RAMNIT BOTNET**

Symantec [says](#) that Ramnit has been around for over four years, first originating as a computer worm. According to the anti-virus firm, Ramnit is a “fully-featured cybercrime tool, featuring six standard families...”

We believe the bot is dismantled...

No new Ramnit flies have been observed. Infected computers still need cleaning.

<table>
<thead>
<tr>
<th>Families</th>
<th>Encounters</th>
<th>Actives</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>ramnit</td>
<td>568,280</td>
<td>18.5%</td>
<td>1.5%</td>
</tr>
</tbody>
</table>
Campaign playbook
Campaign process

Initiation

CME member(s) initiate campaign
- Pick malware
- Initial malware investigation

Formation

Members respond
- Form the group
- Select campaign leader

Plan

Feasibility Study & Plan
- Strategy defined: tactics, and metrics defined
- Team rounded out to fill gaps

Execution

Campaign Begins
- Regular check-ins
- Build, measure, learn
- Adjustments as necessary

Review

Campaign Ends
- PR (if desired)
- Post-mortem, lessons learned
- Success measurements
Initiation

“Let’s eradicate this malware!”
Formation

Call for Participation
• Creates visibility
• Great source of information

Selectively build a group
• Expedites the decision making process
• Add group members as needed

Law enforcement as a partner
Communication

- Document sharing
- Sample sharing
- Conference software
- Secure email communication
Building the plan: Identifying malware's attack points

Reconnaissance
- What sources does the malware use to reach victims?
- How are malware "tested" and packed?

Malware development
- Who are the actors?

Distribute and vector
- How do they infect their victims?
- What else is in the infection chain?
- How diverse is the infection chain?

Command and control
- Does it remotely control the boxes?
- Are there C&C servers? P2P?

Monetization model
- How does it monetize?
Defining goals

Set an end goal
- Disrupt & remediate
- Put attackers behind bars
- Build intel to stay ahead of the curve

Build a timeline
- Campaigns can go on forever
- May deal with a moving target
- Iterate
Campaign state

- In progress
- Stalled
- Failed
Build the plan

- Ethical considerations
- Stakeholders

How do you do X?
Building the plan: Develop a joint PR plan

• Does your org want to be publicly tied to this effort/operation? When will this happen?
• Do you plan on pushing out any form of outward communications around this operation?
• Do you have a dedicated person or team to handle PR/Outward coms? Who are they?
• Do you plan on attributing these threats to any organization or part of the world?
• Do you plan on doing any media interviews, or responding to media inquiries about this op?
Abuse notification

Build templates and process around abuse notification

Incorporate explicitly what should/shouldn’t happen
Success

Impact to the family
Impact to the ecosystem
Impact to my ecosystem

MSRT family CCM (infection rate per 1k)

% of real-time protection customers that encountered this family
Post mortem

Assess each phase
• Planning
• PR
• Etc.

Focus on the good and bad

Involve all campaign members

Communicate learnings to VIA membership