...And You Will Know Us By The Trail Of Our Logs

Malware Research and Analysis Using Log Data

Zachary Wolff, Professional Services Engineer

TakeDownCon, Dallas. May, 18th 2011

Log Analysis Use Cases

- Forensic Malware Investigations
- Detecting Malware
- Comprehensive Understanding of Malicious Software

Example: CVE-2010-3654

- Allows Remote Attackers To Execute Arbitrary Code
- Malicious PDF's seen using this exploit
- Often Generates Similar Event In Windows App Log

3/24/2011 8:16 PM TYPE=Error USER= COMP=XXXXX SORC=Application Error CATG=(0) EVID=1000 MESG=Faulting application acrord32.exe, version 9.3.0.148, faulting module unknown, version 0.0.0.0, fault address 0x6753e2ed.

Example: Gumblar Botnet

- Steals Passwords and/or Installs Rogue AV
- Stolen FTP Credentials Used To Infect Webservers
- Encoded Javascript Injected Into Legit Pages
- P2P Style Infection/Upload Technique

Gumblar FTP Log

Jan 8 06:15:38 x4ilofZ04r pure-ftpd[25107]: (ftpuser@213.171.221.32) [NOTICE] html/Website//administrator/components/com_config/views/application/tmpl/index.html downloaded (44 bytes, 77.42KB/sec)

Jan 8 06:15:44 x4ilofZ04r pure-ftpd[25127]: (ftpuser@213.171.221.32) [NOTICE] html/Website//administrator/components/com_config/views/application/tmpl/index.html uploaded (1175 bytes, 3.72KB/sec)

Jan 8 06:15:50 x4ilofZ04r pure-ftpd[25155]: (ftpuser@213.115.141.21) [NOTICE] html/Website//administrator/components/com_config/views/component/index.html downloaded (44 bytes, 88.24KB/sec)

Jan 8 06:17:38 x4ilofZ04r pure-ftpd[25757]: (ftpuser@88.208.229.173) [NOTICE] html/Website//administrator/components/com_config/views/component/index.html uploaded (1175 bytes, 3.76KB/sec)

Jan 8 06:17:42 x4ilofZ04r pure-ftpd[25789]: (ftpuser@69.59.28.23) [NOTICE] html/Website//administrator/components/com_contact/index.html downloaded (44 bytes, 78.70KB/sec)

Jan 8 06:17:44 x4ilofZ04r pure-ftpd[25812]: (ftpuser@74.208.46.24) [NOTICE] html/Website//administrator/components/com_contact/index.html uploaded (1175 bytes, 8.40KB/sec)

Jan 8 06:18:07 x4ilofZ04r pure-ftpd[25959]: (ftpuser@74.208.166.27) [NOTICE] html/Website//administrator/components/com_contact/elements/index.html downloaded (44 bytes, 86.45KB/sec)

Jan 8 06:18:28 x4ilofZ04r pure-ftpd[26078]: (ftpuser@174.36.185.18) [NOTICE] html/Website//administrator/components/com_contact/elements/index.html uploaded (1175 bytes, 16.46KB/sec)

Jan 8 06:18:54 x4ilofZ04r pure-ftpd[26198]: (ftpuser@91.135.229.250) [NOTICE] html/Website//administrator/components/com_contact/helpers/index.html downloaded (44 bytes, 92.22KB/sec)

Jan 8 06:18:56 x4ilofZ04r pure-ftpd[26215]: (ftpuser@74.208.166.27) [NOTICE] html/Website//administrator/components/com_contact/helpers/index.html uploaded (1175 bytes, 8.44KB/sec)

Jan 8 06:19:43 x4ilofZ04r pure-ftpd[26399]: (ftpuser@88.208.229.24) [NOTICE] html/Website//administrator/components/com_contact/tables/index.html downloaded (44 bytes, 89.88KB/sec)

Example: Zbot In Motion

Dear Prospective Employer,

I applied for your position last week. Could I get an update on my application? Your cooperation will be appreciated in this matter. My resume for your review is http://www.careerbuilder.com/ShareInfo/Resume.aspx?DID=XF69GKN.

Best regards,
Mark Bandol

CareerBuilder Linked To

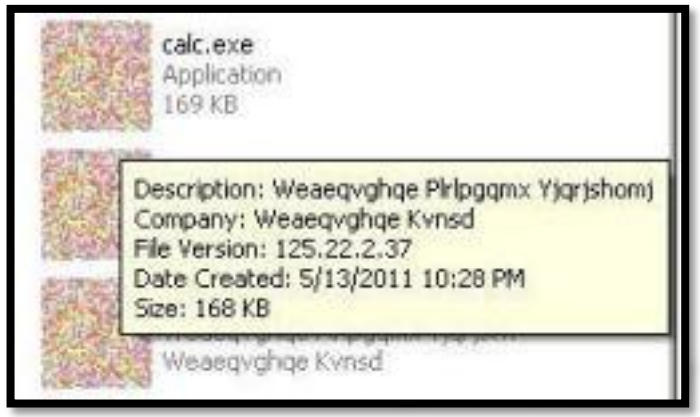
http://payrollserversinstall.com/forum.php?tp=1773b5fa2053528f

Domain Name :
payrollserversinstall.com
Creation Date : 2011-04-18 09:24:17
Updated Date : 2011-04-18 09:24:17
Expiration Date : 2012-04-18 09:24:17
Registrant:
Organization : Liu Jun
Name : liujun
Address : Shang Hai
City : Shang Hai
Province/State : Shanghai
Country : cn
Postal Code : 200085
Administrative
Contact: Name : liujun
Organization : Liu Jun
Address : Shang Hai
City : Shang Hai
Province/State : Shanghai
Country : Shang Hai
Postal Code : 200085
Phone Number : 86-213-2897833
Fax : 86-213-2897833
Email : yazhang2781@hotmail.com

http://payrollserversinstall.com/forum.php?tp=1773b5fa2053528f

Encoded Javascript Downloads And Executes Malicious PDF in the background.

CVE-2007-5659
CVE-2008-2641
CVE-2008-2992
CVE-2009-0927



Malware Log Trail

- Email Server
- Anti-Spam
- IDS/IPS
- AV Logs
- Event Logs
- Router/Firewall
- Proxies
- Authentication Logs (VPN's, DC's)

LogRhythm®

Pro-Active Malicious Log Collection (darknets)

- Routable Network Segment, No Legit Devices
- Honey Potted Network Shares
- ….