Monthly Research

Linuxマルウェアについて

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

はじめに

- サーバ、モバイル、組み込み機器とLinuxが利用されているプラットフォームは大幅に増加している

- Linuxマルウェアが増加中
  - 2015/01/19から01/26までにVirusTotalに投稿されたELFファイルは127385個（Win32ファイルが2722106個）
  - ただし、これらがすべてマルウェアというわけではない

- 今回のMonthly ResearchではLinuxマルウェアの最新事例を紹介し、傾向について考察する

ELF DDoS botnets（Chinese Chicken）

- 2011年頃から観測されている、中国語圏で開発されていると思われるマルウェア
  - botconf2014にて、Peter, Jaromírらが詳しく報告している https://www.botconf.eu/chinese-chicken-multiplatform-ddos-botnets/

- 主に中国語圏のオンラインゲーム、オンラインショップ、フォーラムがターゲットになっており、DDoS攻撃による脅迫などに使われている

- 代表例
  - IptabLes/IptabLex
  - XOR.DDoS
  - AES.DDoS
  - ChinaZ

IptabLes/IptabLex (2013~)

- Akamaiが詳細を報告している、DDoS攻撃を行うELFマルウェア
- Apache Struts、Tomcat、Elasticsearchなどの脆弱性を用いて攻撃対象に侵入
  - 最新の脆弱性を取り入れている

- /boot 以下に .IptabLes または.IptabLeというファイル名で自身を格納
- C&Cサーバに接続し、DDoS攻撃の攻撃ノードとなる

参考:
"IptabLes and IptabLex DDoS Bots Threat Advisory", September 3, 2014
http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-iptables-iptablex-linux-bots-botnet.html

XOR.DDoS (2014~)

- Linux向けELFマルウェア
- LKM（Linux Kernel Module）ルートキットが含まれている
  - “Suterusu”と呼ばれるオープンソースな LKM rootkitに特徴が似ている
- もしインストールされてしまった場合、プロセス隠ぺい、ファイル隠ぺいなど、ユーザーモードマルウェアに比べて発見、対応が難しくなってしまう

参考:
"IptabLes and IptabLex DDoS Bots Threat Advisory", September 3, 2014
http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-iptables-iptablex-linux-bots-botnet.html

AES.DDoS (2014~)

- 様々なアークテクチャで動作することが確認されているELFマルウェア
  - EM_386, EM_x86_64, EM_MIPS, EM_ARM, PE x86のバリエーションが確認されている
  - MIPSはルータなどでよく利用されているアークテクチャ

- 攻撃対象をサーバに限定せず、デスクトップ、ルータ、IoTデバイスも侵入し、DDoS攻撃の踏み台にするためのマルウェア

参考:
“MMD-0026-2014 - Router Malware Warning | Reversing an ARM arch ELF AES.DDoS (China malware)”,
http://blog.malwaremustdie.org/2014/09/reversing-arm-architecture-elf-elknot.html

ChinaZ (2015~)

- shellshock脆弱性を使ってサーバへの侵入を試みる、DDoSボットネット関係のELFマルウェア

参考:
“MMD-0030-2015 New ELF malware on Shellshock: the ChinaZ”,
http://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html

Linuxマルウェアの傾向

- Windows向けのマルウェアほど洗練されているわけではない
  - しかし、アンチウィルスベンダーがWindowsに注力している関係で、商用ソフトでも検知率はさほど高くない
  - “Google's VirusTotal puts Linux malware under the spotlight” http://www.zdnet.com/article/googles-virustotal-puts-linux-malware-under-the-spotlight/
  - カスタマイズされたUPX圧縮を用いるなど、今後Win32マルウェアのように洗練されていく可能性がある
- クロスプラットフォーム性という、Windows向けマルウェアにはない性質が垣間見える

References:
“Golangによるマルウェア(Japanese)”, http://blog.0day.jp/2014/09/linuxgoarmbot.html

Linuxシステム上のマルウェア検知&侵入検知

- ClamAV、Linux Malware Detect等を用いたマルウェア検知
- AIDE等を用いたファイル改ざん検知
- Linux IMA(Integrity Measurement Architecture)を用いた実行ファイルの改ざん検知
  - カーネルレベルでプログラム実行を監視し、改ざんされたプログラムの実行を検知する

攻撃緩和策

- SELinuxによるアプリケーションの隔離
  - 被害範囲を局限できるが、根本的な対応となるわけではない
- ファイヤーウォールによる“外向き”の通信制限
  - Command and Controlサーバに繋げなければ、基本的にbotは機能しない

まとめ

- サーバ、モバイル、組み込み機器とLinuxが利用されているプラットフォームは大幅に増加しており、それを攻撃対象とするマルウェアによる大規模な攻撃事例が観測されている
- ソフトウェアの脆弱性をついて一方的に侵入、乗っ取りを行うようなマルウェアが迅速に開発されて攻撃を行ってくる
- システムが利用しているソフトウェアすべてを把握し、迅速に対応する必要がある
  - 同時に、攻撃や侵入を受けた場合の検知と、対応まで攻撃を緩和する仕組みを検討すべきである

参考文献

- “virustotal += Detailed ELF information” http://blog.virustotal.com/2014/11/virustotal-detailed-elf-information.html (2015/01/26 viewed)
- “VirusTotal/Statistics” https://www.virustotal.com/ja/statistics/ (2015/01/26 viewed)
- “Linux DDoS Trojan hiding itself with an embedded rootkit” https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
- Linux-Malware−Detect https://www.rfxn.com/projects/linux-malware-detect/
- Linux-IMA http://sourceforge.net/p/linux-ima/wiki/Home/

Contact Information

E-Mail : research—feedback@ffri.jp
Twitter : @FFRI_Research