FROM FOG COMPUTING TO ROP GADGETS

FELIX LEDER
Felix.leder@bluecoat.com

OVERVIEW

- Threat Landscape
  - Adversary
  - Cyber
  - 0-day
  - APT
  - HVT
- Targets
  - BYOD
  - Internet of Things
  - Cloud
  - Fog
  - ADS
- Preparation
  - MSSP
  - MDM, MAM, MM
- Protection
  - Crowd
  - AED (advanced evasion detection)
  - NGFW
- Detection
  - SIEM
  - Real Time Data Analytics (Big Data)
  - Threat Intelligence, OSINT
  - C2
  - G2
- Exploitation
  - ROP Gadgets, ASLR, DEP
- Post-Breach
  - DLP, Exfiltration Prevention/Detection
  - eDiscovery

OVERVIEW

- Threat Landscape
  - Adversary
  - Cyber
  - 0-day
  - APT
- Targets
  - BYOD
  - Internet of Things
  - Cloud
  - Fog
- Preparation
  - MSSP
  - MDM, MAM, MM

THREAT LANDSCAPE

- "Guns don’t kill people, people kill people" [NRA]
  - Tools don’t break into your systems, organizations do

ADVERSARY

- Who has an interest in breaking into your system?
  - Hacktivists
  - State Sponsored
  - Cyber Criminals

STATE SPONSORED

- Origin: “controlling well” but lost meaning
- ... space – Internet
- ... crime
  - Banking, click-fraud, DDoS, spam, break-in
- ... war / warfare
  - DDoS, espionage, sabotage
- ... terrorism
  - Same as warfare but non-state (depends on view)
- -hate, -pilgrimage, -sex, -security

CYBER...
Russia-Ukraine Standoff Going Online as Hackers Attack

By fantastic news, by fantastic news and Aaron Krasic - Oct 5, 2014 6:31 PM EDT - 10 comments

Cyberspace is fast becoming a battlefield for Ukrainians and Russian hackers as they try to exploit vulnerabilities on the desktops and servers of state-owned and private entities.

Hackers have launched attacks on the websites of state agencies and publications on both sides. A Russian government hacking initiative has ordered a shutdown of the Ukrainian state's websites and a Ukrainian government hack that took down state media.

0-day vulnerability: vendor not yet notified
0-day malware: No antivirus detection

[Graph showing antivirus detection rates]

• ADVANCED PERSISTENT THREAT - APT

Advanced?
- nay (nearly invisible)

Persistent?
- yep (long-term)

Threat – uh oh

⇒ There is no 100% security ("just need firewall + AV" is long ago)

• HIGH VALUE TARGET - HVT

SCADA
ICS


• TARGETS

Tablets
Smartphones
Laptops

Bring Your Own Device
- Full mobility ⇒ agility
- (Company) cost saving
- Productivity through familiarity (spare time)

Challenges:
- Easy to get lost/stolen
- Full data access
- No control over work infrastructure
- Isolated down (hard to add security monitoring)
- Policy enforcement

Last but not least: Privacy
INTERNET OF THINGS

- Locked devices
  - No patch
  - No modifications possible
- Full Internet Connectivity
  - Attackers can exploit
  - Multi-platform attacks

Cloud = The Internet

I don’t care where the service is…
... as long as it works seamlessly
... scalable to multiple users
... access from (almost) everywhere

- IaaS, PaaS are usually “the cloud”

CLOUD

Cloud = The Internet

I don’t care where the service is...
... as long as it works seamlessly...
... scalable to multiple users...
... access from (almost) everywhere

- IaaS, PaaS are usually “the cloud”

FOG COMPUTING

- Local “cloud” (used to be called data center)
- or service close endpoints (edge computing)
- Reduced latency
- Local data transfer
- Process locally instead of sending to the cloud
- Local availability of typical cloud services
- Using closest/“own” infrastructure

AAS

- ... as a Service (aS)
  - Cost efficient
  - Leave domain to experts (hopefully)
  - Leave your data to somebody else

- Infrastructure as a Service IaaS
  - Routers, VMs, IP addresses, SAN

- Platform as a Service - PaaS
  - Full platform
  (LAMP, Hadoop clusters, ElasticSearch, Tomcat, Django, SQL server)

- Software as a Service (SaaS)
  - Office 365, Google docs

PREPARE

... your defenses

MSSP / UTM

- Managed Security Service Providers
  Manages security for you
- Another aS: Security as a Service

- A.k.a. Unified Threat Management
  - Firewalls, Web Filtering, NGFW, IPS, IDS
  - Endpoint security, AV
  - VPN, WAN, WiFi, Patch Management
  - Incident handling

- Sometimes PaaS
MDM, MAM, MIM

• Mobile DEVICE Management
• Mobile APPLICATION Management
• Mobile INFORMATION Management

WORKING WITH BYOD

• Mobile DEVICE Management
  • Rollout of policies, settings
  • Monitoring / device portfolio / rooted devices
  • “Remote wipe” / lock
  • Backup

• Mobile APPLICATION Management
  • Trusted apps
  • Installed apps
  • “Wrapped” apps to limit data access

MOBILE INFORMATION MANAGEMENT

http://www.sudcamp.com/best-free-dropbox-alternatives/

PROTECTION

CROWD

• Power of the people
  • Exploit existing client base (there is nothing like a free lunch)
  • Pay small money to a lot of people to do a lot of work

• Crowd Intelligence
• Crowd AV
• Crowd Testing
• (Crowd Funding)

ADVANCED EVASION DETECTION

• Stream reassembly is not trivial
• And not rocket science
NGFW – NEXT GENERATION FIREWALLS

- Application identification by protocol details
  - Usually http based protocols
  - Extend traditional IP, port, protocol, fields, ...
    model
- Application level IPS
- User identification

AV - ANTI-VIRUS

- Most misunderstood
- Common perception: Something that applied signatures to files
- Most AV suites have more:
  - On-access detection
  - Clean-up
  - Firewall
  - HIDS, HIPS

DETECTION

- Security Information and Event Management
  - Collect
  - Aggregate
  - Correlate
  - Alert
  - Keep data for future (forensic) analysis

REAL TIME DATA ANALYTICS

- Previously known as BIG DATA
- Research and solutions around for 50 years
  - Divide and conquer (now known as map-reduce)
  - Data indexing
  - Multi-processing
- Problem now: “Store everything”-mantra
- Now there are easy-to-use tools
  - Hadoop
  - Elastic Search
  - Solr
  - Logstash / Kibana

THREAT INTELLIGENCE

- Threat Intelligence
  - Black lists, white lists, reputation scores
  - Spam templates
  - Intelligence as a Service (whois, detection history and correlation)
- OSINT – Open Source INelligence
  - Public Sandbox reports
  - CIA world fact book
  - Open directory listings on C2 server
**38 NORTH**

- Military grade intelligence
- Related to military units

**C2 a.k.a. Command & Control**
- Controlling instance of botnets
- Also: Drop zone

---

**EXPLOITATION**

- **Stack**
  - Function 1
  - Function 2

- **Return addr.**
- **Buffers**
- **Shellcode**

- **Data Execution Prevention**

---

**RETURN ORIENTED PROGRAMMING**

- **Process Space**
- **ROP chain**
- **Kernel32.dll**
- **Lib.so**

- **Modified return addr.**
- **Junk**

---

**ADDRESS SPACE LAYOUT RANDOMIZATION**

- **ASLR**
  - DEP & ASLR active in most modern OS
  - Latest Windows (limited)
  - iOS 4.3+
  - Android 4.0+
  - OS X 10.5+
POST BREACH

DLP / EPS / EDS

- Data Leakage/Loss Prevention
- Extrusion Detection/Prevention System

- Possible monitoring points
  - Endpoint
  - Network
  - Storage

- Sophistication varies widely
  - Log access, transfer
  - Signatures for content
  - Digital signatures / watermarks
  - DRM

E-DISCOVERY

- E-Discovery
  - Network forensics
  - Host forensics
  - G2 + OSINT

1 Minute Advertisement

INTEGRATED

SSL Visibility

- Blue Coat SSL Visibility Appliance
- ThreatBlade Analysis Appliance

Security Analytics Platform by ThreatBlade

Security Analytics Appliances
Security Analytics Storage
Security Analytics Central Manager

A Complete and Integrated Portfolio of Modern Advanced Threat Protection Solutions

SUMMARY

- There is a lot of hype
- Who is your “adversary”?
- Have tools to protect and to detect
- Breaches will happen – be prepared for the incident