RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: AIR-W05

Sustaining a Malware-Free Enterprise Network

Sunil Varkey

Chief Information Security Officer
Wipro

@sunilvarkey

#RSAC

Impact

- Multi Billion $ impact globally across industries
- ‘Trust’ is questioned
- Business disruptions
- IP Theft
- Legal / contractual liabilities

All industries fall victim to cybercrime through malware in different degrees
Cost of cyber crime is increasing every year

WIPRO
Applying Thought

Malware

Software specifically designed to operate in a malicious, undesirable manner to disrupt, intercept, control or damage a computer (IT) system without user consensus

Types

Adware, Backdoors, Bots, Browser Modifiers / Hijacker, Bugs, Downloaders & Droppers, Memory only, Obfuscators & Injectors, Password Stealers, PUP, Key loggers RAT, Rootkits, Ransomware, spyware, Trojan horses, viruses and Worms

Delivers, distributes, infects, exploits, extracts information, destruct

Actors & Motive

Actors

- Cybercriminals
- Terrorist / Insurgents
- Hacktivism / Patriotism
- Script kiddies
- Cyber-researchers
- Advanced / Rogue States
- Competition

Motive

- Financial damage
- Disruption or control
- Espionage
- Fraud / Corruption
- Blackmail / Sabotage
- Access to data
- Traffic generation

Prioritization

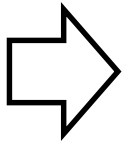
- Target Systems
- Propagation methods
- Motive
- Capabilities
- Risk

Varies between Industry, service and Geo locations

Type of compromise & Propagation vectors

Transmission Vectors

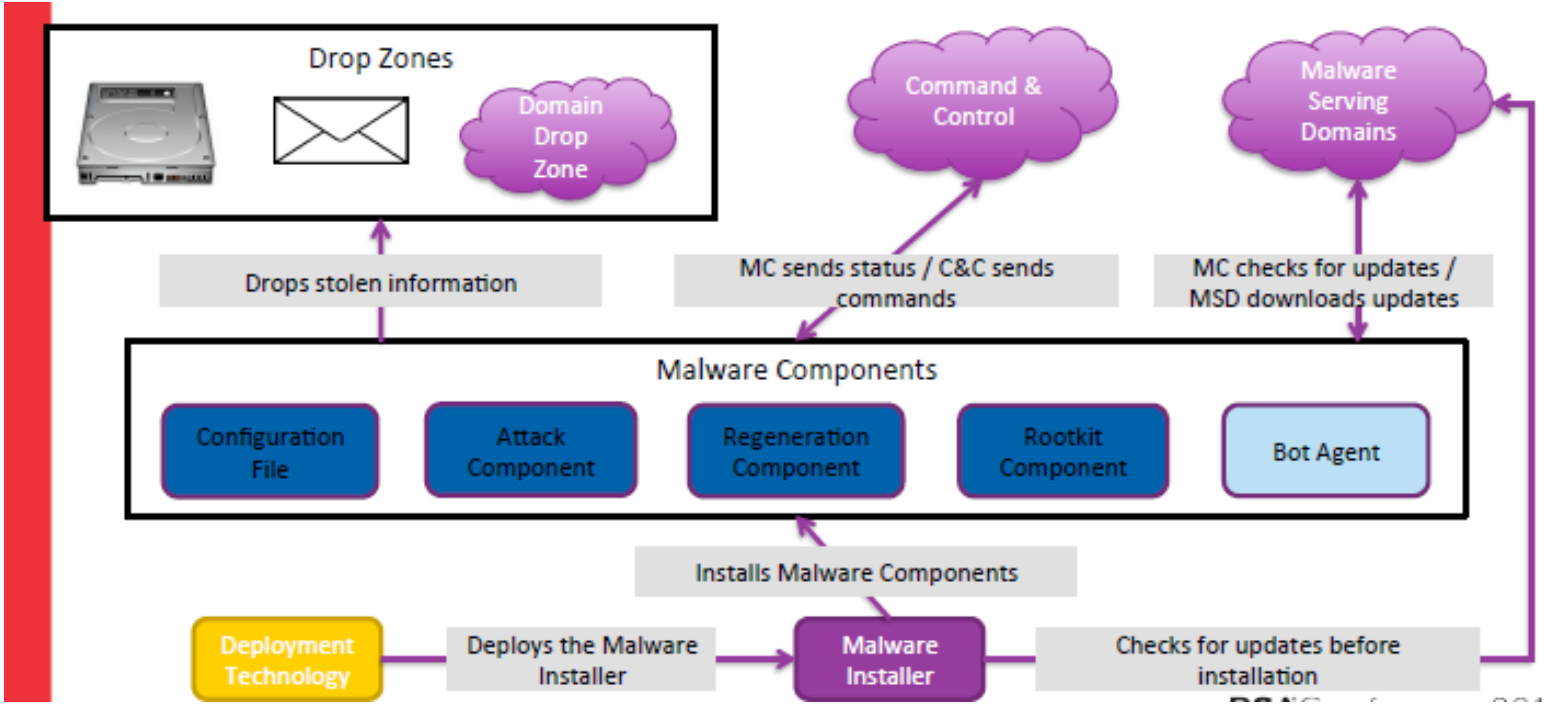
- External Storage Media
- Emails - smtp
- Websites – http(s)
- Network
- Applications / package



- User Tricked / Deception
- Auto Run
- Vulnerability / Misconfiguration Exploit
- Macro / Malicious Scripts
- Password Brute Force
- Zero-Day
- Drive-by download

WIPRO
Applying Thought

Attack Infrastructure (behind the scene…)



Christopher Elisan – Malware, Rootkits & Botnets – A Beginner's Guide (McGraw-Hill Professional
Demystifying a malware attack" by Chistopher Elisan - RSA Conference 2016

Attackers (behind the scene…)

Sponsor
- Government
- Commercial Organization
- Non-commercial Organization
- Activist Groups
- Individual
- Terrorist Organization

Crime Boss
- Runs the show
- Individual or organization
- Middle man between sponsor and TPs
- Can be a sponsor

Money Mules
- Unsuspecting Public
- Work from home

Malware Writers
- Original malware creator(s)
- Offer malware "off-the-rack" or custom built
- May offer DIY construction kits
- Money-back guarantee if detected
- 24x7 support

Botnet Master
- Individual or criminal team that owns the botnet
- Maintains and controls the botnet
- Holds admin credentials for CnC

Botnet Operator
- Operates a section of the botnet for direct financial gain
- Issues commands to the bot agents
- May be the Botnet Master

Deployment Provider
- Specialized distribution network
- Attracts and infects victims
- Global & targeted content delivery
- Delivery through Spam/drive-by/USB/etc.
- Offers 24x7 support

Resilience Provider (MSP)
- Provides CnC resilience services
- Anti-takedown network construction
- Bullet-proof domain hosting
- Fast-flux DNS services
- Offers 24x7 Support

Demystifying a malware attack" by Chistopher Elisan - RSA Conference 2016

Phases of Attack

- Target Identification and selection
- Exploit Discovery and Configure
- Distribute and Deliver
- Execution of Attack - Infect and Exploit
- Malware Propagation
- Collection of Credentials / data / control

- Commodity
- Sophisticated
- Targeted

Is Malware worth a threat for focused defense?

Can we defend?

Impact of Malware in Enterprise

- Data Exfiltration
- Untrusty computing environment
- High volume of abnormal traffic leading to network performance
- High potential of sensitive data and credential in public forums
- Low performing IT systems
- Service interruptions
- Contractual and Legal liabilities
- Reputation damage

WIPRO
Applying Thought

Direct cost of malware

- Roughly $120 per malware infection
  - At least 5 resources involved in handling the entire lifecycle of a malware infection from detection, analyzing, alerting, containment to remediation
  - Impacted system user and support engineer to spend 2 hours on this (avg cost of $20 per hour per person)
  - License cost of events per second in correlation and Big data platform
  - Events storage cost at various systems and technology

Average cost of $4000 / day to keep network clean from malware

WIPRO Applying Thought

Vision

Build a sustainable solution for centralized control and granular visibility of malware lifecycle at enterprise level, capable of effective and timely detection and containment, leading to a near zero malware enterprise IT environment.

Key Challenges

- Sophisticated and Dynamic malware's
- Complicit and insensitive users
- Misaligned configuration and policy non compliances
- Vulnerable systems and network
- Lack of / inadequate layered security controls and on external devices, access and privilege ID's

Malware considered to be part of the IT environment,

Approach

- Build use cases based on risk and impact for stakeholder buy in
- Inventory and baselining
- Malware profiling
- Define Detection, Analysis and mitigation process lifecycle
- Technology stack optimization
- Influencing / controlling malware events

People – Process - Technology

Predictive – Prevention – Detection – Containment - Remediation

Baselining

- Prevalent malware presence and root cause of incidents
  - Family
  - Propagation Vectors
  - Users / Locations
- State of vulnerabilities and misconfiguration in the network
- Incident handling process procedure documentation and practice review
- EOL, PUP, Non Standard software's
- User access privileges

People

- Acceptable usage policies
- Security vs Convenience
- User behavior & Sensitivity
- Level of Security Awareness
- Policy compliance

Information security is My Responsibility

Process

- Effective Vulnerability Management
- Configuration Policy / Hardening enforcement
- Proxy / external drive / Administrative privilege governance
- Noise reduction, Contextualization and baselining
- Inventory and control coverage
- Analytics & Monitoring
- Standard incident handling – response process across enterprise

Continues Management support

Malware profiling

- Target – Individuals / business segments / technology / Geo locations
- Motive – Credentials, PII, IP, Ransom
- Known / Unknown malware
- Propagation Vectors
- Platform / Technology
- Persistency

Malware / Incident Analysis

- Malware type & Family
- Behavior / Pattern / Indicators
- Hash Value, Call back pattern / URL's
- Impacted systems / user
- Source / Target
- Dropped files / Scripts
- File path / Registry changes
- Propagation vector

WIPRO
Applying Thought

Indicators of Compromise

User

- Slow down
- Pop Up
- HDD Space issues
- New home pages
- Antivirus alerts
- Files not accessible

Incident Handler

- Call back
- Registry Changes
- Network and ports traffic pattern
- Denied traffic
- Suspicious HDD / NW activities
- Threat intelligence

Call back detection

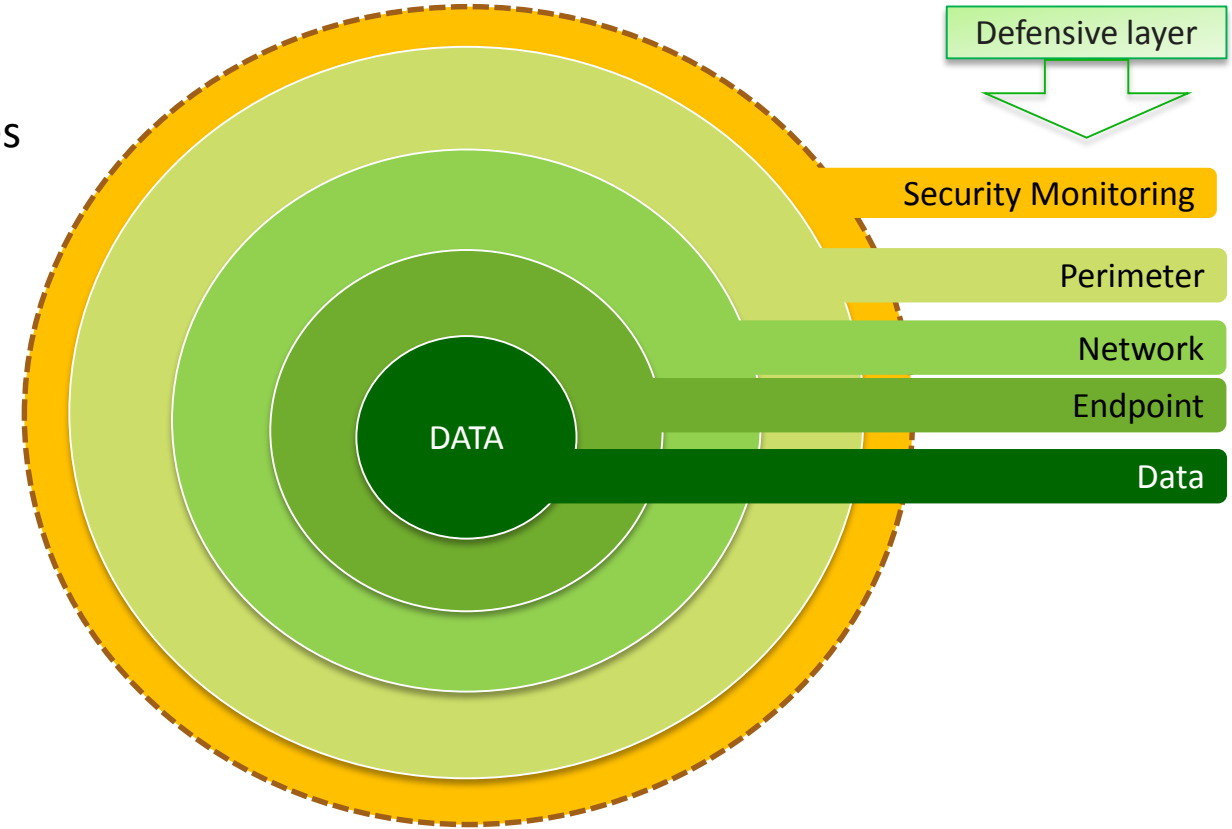
- Track suspicious outbound traffic from Web Proxy
- Tune Network Firewall and Intrusion Prevention Systems
- Use Threat Intel and configure alerts in SIEM to provide data on known command-and-control IOC
- DNS log, outbound denied and abnormal traffic analysis across controls

Technology

- Leverage layered security controls at perimeter, network and end point to detect and contain malware events
- Enable global threat intelligence feeds (ex. GTI, Wildfire) for validation of newer threats in the cloud database
- Network level sandboxing of files and Tight integration between security controls to share data with Antivirus and IPS layers for containment of new malicious files

Security Control Landscape..

SIEM
Log Vaults
Layer3 Switches
WAF
DLP
SSL Gateways
Decryption
PIM
IdM
Threat Intel
Spam filters
Web Filters
NAC / NAP



Firewall
Perimeter IPS
Proxy
Routers
Switches
WIPS
DDOS
Antivirus
Sandboxing
Encryption
HIPS
Network IPS
DNS
VA

WIPRO
Applying Thought

Key Technology controls

- Antivirus
- Proxy
- IPS / HIPS
- Spam Filters
- Firewall
- Sandboxing
- Threat Intelligence
- Zero-day Threat Protection
- ATP / Behavior based solutions

Signature vs Behavior based Anti-Malware

- Known definitive Hash value
- Finger print (partial) Byte-Signatures
- Binary Diffing
- Generic

- **Only known malware**
- **Response lag**

- Heuristic - API hooking, sand-boxing, file anomalies etc
- Abnormal or suspicious behavior
- Alter hosts files, Privilege, Registry
- System files in different path ex. autorun.inf

- **High False positives**
- **More people, resource**

Solutions should compliment

WIPRO
Applying Thought

SMTP

- Perform email pattern analysis to detect anomalies
- Specific rules to filter / flag / Quarantine suspicious mails
- Threat feed integrations – Blacklisted IP's, spamming domains
- Allow only business attachment
- SMTP level antivirus scanning
- Block known suspicious and malicious file extension at email gateways (in addition to executable, JS files, .wsf files, .vbs, .wsh etc)

HTTP

- URL categories related to security, malware, malnet, phishing, malicious outbound, botnet, sources, placeholders, phishing, p2p, PUP, RAT to be restricted and monitored
- Uncategorized URL category to be blocked and monitored
- Software / file download should pass through antivirus scanning
- Web browsing control / governance while connected outside office network

Around 30% of malware incidents occur outside office timing / network

Firewall - IPS

- Service based rules rather than port based rules at firewall
- All known malware ports to be blocked and monitored
- Protocol based inspection at IPS – perimeter and internal
- Code, anomaly, reputation analysis using IPS
- HIPS enabled to block monitor abnormal calls, executions and activities

AV

- End point, Network, Storage, Web / Email Gateways
- N-2 Engine, minimum 3 day old signatures
- All features including AV, HIPS, Firewalls, Device controls enabled
- Real time scan ON, schedule scan once in a month
- Advance malware protection on end points and at network layers
- Capable to quarantine infected system if required
- Continues optimization to improve auto clean ratio
- Real time scanning to identify rouge systems, failed - corrupted AV agents

Ransomware

- Block suspicious and malicious file extension at email and Web gateways (in addition to executable, JS files, .wsf files, .vbs, .wsh etc)
- Disable macro execution in Microsoft Office documents
- Analyze web traffic to detect dropper files
- Use built-in file versioning services like Windows Volume Shadow Copy
- Use Host IPS to detect,
  - Flag operating system calls made to encryption processes
  - Flag processes that read or write too many files too quickly
  - Flag processes that change files' entropy values

Whitelisting vs Blacklisting

- Application control enforcement on critical systems
- Digital signature based whitelisting
- Process to review internal developed applications / scripts to whitelist
- Hash values / blacklisted IP ranges are dynamic in nature

Governance

- ISMS should have formal policies and procedures against risk of malware
- Defined process and procedure to monitor, analyze and contain malware through its lifecycle should be operationalized
- Technical controls & configurations should be periodically assessed and documented, all changes should follow required process
- There should be clearly defined management procedures defining responsibilities and accountability for dealing with malware incidents, containment and recovery
- Cyber threat related to malware should be part of BCP / DR plan

Metrics provide the means by which to build excellence, they can serve as early warning signals or they can justify or negate the spend an organization can make

Metrics..

- Total number of malware / day
  - Desktop, server, laptop, storage
- New malware presence on that day
- Top 10 malware details
- Infected system user details
- Propagation vector
- Malware detected at signature less solution
- No. of IPS signature on malware in block mode vs monitor vs total
- Web / FW traffic blocked – outbound
- URL Category
  - User / Attempt count
- Spam mail count
  - Total, blocked, allowed
  - Analysis of the spam mails

Coverage of Antivirus & Posture

Ongoing basis

- Continues monitoring at various security control layers for indicators
- Periodic baselining
- Optimization of security controls based as a dynamic activities
- Engagement of users and stakeholders in sustenance
- Periodic measurements of baseline deviations for early warnings and program performance indications

Time to detect and contain is critical, ensure sense of urgency at all time

Thank You

Sunil Varkey
CISSP, CIPP/US, GSNA, CISA, CGEIT, CRISC, ABCP, *ITIL- V2 (Red Badge) & Six Sigma GB certified*

Twitter: @sunilvarkey
Sunil.varkey@wipro.com