Introduction

Christopher Day

- Joined Terremark December 2005
- Chief Security Architect
- Responsible for Terremark's global information security services
- Have led numerous projects around the world ranging from large-scale incident response and forensics to vulnerability assessments and penetration testing

Agenda

- Who is Terremark?
- Intrusion Suppression
- Challenges
- Conclusion and Questions

Terremark Facilities

NAP of the Americas

- 750,000 square foot purpose-built data center
- The most connected hub in the world; switching 90% of traffic to/from Latin America to rest of the world
- Global connectivity from >160 carriers
- 100% SLA on power and environmentals; significant access to power

Strategic Global Footprint to Deliver Services

Compliance

- We must adhere to, or provide support for, a number of control and compliance frameworks:
    - SAS Type 2
    - PCI
    - ISO 27001
    - FISMA
    - DIACAP
- Now that we are a Verizon subsidiary, the scope is increasing greatly

Security Services Portfolio

Managed Security Services

- Managed Firewall
- Intrusion Detection/Prevention
- Log Aggregation and Correlation
- Network Traffic Session Monitoring and Analysis
- Full-packet capture and attack replay
- Network Forensics
- Data Leak Detection/Prevention
- Rapid deployment ‘SOC in a Box’ and cloud based ‘SOC in a Box’

Engagement Services

- Incident Response
- Digital Forensics
- Vulnerability Assessment
- Penetration Testing
- Compliance Support

Effective Information Security - What Problem Are We Trying to Solve

Effective Information Security = (**A**dministration and **C**ompliance) + (**T**hreat **A**wareness, **A**ssessment, and **M**itigation

Intrusion Suppression

- Platform architecture and technology choices primarily designed to support an ***intrusion suppression*** methodology

- ***Intrusion suppression*** assumes that given time, an advanced and persistent adversary will compromise your environment; the goal is to minimize the impact of compromise while denying the adversary further use of their attack vector

- Detect the compromise, not the attack
- Approach is far more realistic and resilient given the complexity of modern IT environments and adversary sophistication

Intrusion Suppression – Requirements

- Visibility is key!
  - If you rely only on signature-based systems and SIM aggregators to tell you when you have a problem in your environment then you are effectively blind with respect to many of today's threats

- Speed is key!
  - The ability to mitigate compromised systems quickly is extremely important
  - A capable, mature incident response capability is necessary
  - What do we mean by 'mitigate' and 'quickly'?
  - If you must wait for your vendor or service provider to react to a sophisticated adversary then you lose

Intrusion Suppression – Requirements

- A threat intelligence capability is key!
  - Don't wait for the bad guys
  - Must be able to process the 'take' from a compromise and make it **actionable**
  - Be able to do your own in-house malware analysis

- So, how do we actually do this and how do we measure success?

Intrusion Suppression – Platforms

- We want to maximize our visibility and automate as much as possible while enabling analysts

Platforms - Voltage

Platforms - NetWitness

Platforms – Voltage + NetWitness

Platforms - Straylight/Malytix

Threat Intelligence

Offense

Intrusion Suppression – “Ecosystem”

Intrusion Suppression – Some Metrics

- Observed attack and threat classification correlated (sanitized, non-attributable) across commercial, Federal government, and military customer network targets
- **Average time to detect compromised systems**
- **Average time to mitigate compromised systems from detection point**
- **Number of 0-day exploits and malware discovered**
- **Threat and malware analytics including network, disk, and memory detection observables**
- Numbers of observed attacks per day, week, and month
- Source Internet Protocol (IP) addresses, source country, and geographical location of observed attacks
- Numbers of mitigated attacks and

mitigation method
- Number of detected compliance violations (FISMA, PCI, etc.)

Intrusion Suppression - Challenges

- This approach isn't easy nor cheap
- Labor intensive
- Very skill intensive (network, malware analysts)
- Must have a capable IR capability to mitigate otherwise you are just "stamp collecting"
- No existing compliance framework requires it so it can be difficult to justify to management
- ROI is hard to quantify (though the Sony breach helps)

- Data reduction is important so as not to drown in an unstructured sea of data

- The number of nodes (sensors, hosts, users, etc.) must not be

Conclusions

- We use the intrusion suppression approach to defend our infrastructure and our customers from compromise
- No guarantees but we succeed more than we fail and can measure

- You must know, or be able to know, your environment (topology, flow patterns, traffic types, encryption in use, protocols) better than an adversary. If not, all is lost.
- Rapidly knowing the capabilities of your adversary's tool chain allows you to know when you can 'fight' through and operate in a 'degraded' state
- Need a strong, fast IR capability for IS to work

Conclusions

- Signatures are the output of the process
  - Rapid Detection by SOC
  - Encapsulation of ‘expertise’

- Questions?