Leveraging Proactive Defense to Defeat Modern Adversaries

Andrew Case / @attrc

Volexity

Black Hat Webcast | September 2015

Why is Proactive Defense Needed?

- Many opaque components of the information infrastructure
- You are combating a creative and adaptive adversary and thus you need a creative and adaptive analyst to find them
- Statistics have shown that people are compromised for years without noticing

VOLEXITY

What is Threat Hunting?

- Searching for adversaries without a particular indicator
- Dedicating time and resources to deep analysis of potentially compromised resources
- See [1] for great commentary by Sean Mason and [2] for several posts by Jack Crook

What are its Benefits?

- Makes the organization proactive against attackers
- Quickly find gaps in system and application configurations
- Defenders more familiar with their own environment and infrastructure

Gaining Familiarity

- Understanding and defining "normal" in order to detect anomalous behavior and attributes

- "normal" is unique to a particular organization and even subsets within the organization
  - "normal" of a web server is quite different than the system of Joe in accounting

- Unfamiliarity with "normal" leads to extremely ineffective response

Running Processes

- If your analysts were given a list of every process running on a system in your environment, how many of them could definitively rule each as normal or abnormal?

- How would this be judged?
  - Name of the process?
  - Path to the executable on disk?
  - Parent process?

- Patrick Olsen has gone through great lengths to document this [5]

Process Privileges

- What privileges do each process run as?
- Do any 3rd party programs abuse privileges or grant themselves higher privileges than necessary?
- Do you know which of your users run as local admin?

Network Activity

- Which applications should be listening for network connections?
- Which applications should talk on the network?
- Is there any ingress/egress filtering?
  - Has it been disabled or tampered with by malware/attackers?

Kernel Drivers

- Kernel drivers have full access to entirety of a system and its resources
- A default Windows 7 install loads over 100 kernel drivers
- Two of the following drivers are normal, two are Stuxnet, do your analysts know which?
  - MRxCls
  - MRxDAV
  - MRxNet
  - MRxSMB

Documentation is Org Knowledge

- Team members should not live in a silo
  - "normal" should be documented in a way that other team members can access
- Documentation outlives employees leaving and scales during incidents
- If your entire IR team mutinied tomorrow, how long would it take for new hires to regain all the departing knowledge?

What is the End Result?

- Proactive detection of threats
- **Effective** detection and response
- IR teams that deeply understand their environment
- Organizational knowledge that continues to grow and survives generations of employees

How Do You Get There?

- The executives need to understand the value of a properly prepared IR team

- The IR team must be elevated to the status of the IT Security team and be just as an integral a part of the organization’s ongoing IT flow

Security vs IR

- Security teams are positioned during all parts of the IT process while IR is used only during incidents
- This leads to IR staff not being effectively utilized and not being an on-going part of the organization

IT Security Pre-Deployment

- Baseline testing of gold images
  - Security evaluations done well before production use
- Application development
  - Secure SDLC
- Secure DevOps
  - Incorporating security into cloud deployments
  - Richard Mogull does great work in this space [3]

IT Security Post-Deployment

- Continuous:
  - Vulnerability scans
  - Penetration tests
  - Application security assessments

IR is Embedded Into Nothing

- It is always after the fact
- This leaves knowledge gaps and forces on-the-spot learning during incidents
- How do we fix this?

Incorporating the IR Team Pre-Deployment

- As security reviews gold images, the IR team should be building baselines and looking for logging misconfigurations that prevent full forensic exploitation
- Applications should be developed and configured so that all relevant activity is logged and recoverable

Incorporating the IR Team Post-Deployment

- Continuous:
  - Threat hunting
  - Documentation of changes to systems and applications
  - Incorporation of new forensics artifacts into analysis processes

Incident Preparedness

- IT security has dedicated systems for vulnerability scanning, application testing, etc.
- IR teams need dedicated, pre-configured systems to effectively hunt as well as respond to incidents

Incident Preparedness Essentials

- Network monitoring
- Dedicated storage servers
- Deployable acquisition/sampling tools and agents
- Analysis servers with real processing power
- Without these and others, response will be chaotic, underpowered, and likely ineffective

Utilizing Documentation

- As the IR team becomes embedded, everything it learns should be documented
- If done correctly, everything that is known from a forensics perspective about a system and its applications will be readily available to all team members

Spending: Security vs IR Preparedness

- If “Shell Shock 2” were to be released right now would you feel better knowing your systems were fully patched (hence vulnerable) or that you had a fully prepared IR team that can handle the outbreak effectively?

- Does your organization’s resource allocation reflect your feelings on this?

Threat Intelligence – The Bad

- Is **not** a replacement for threat hunting, baselining, and a functioning IR process
- Does not scale without the right infrastructure
- When used incorrectly, is no better than AV signatures

Threat Intelligence – The Good

- With good, proactive IR processes in place, TI can *greatly* enhance detection of adversaries

- With supporting infrastructure, mass network sweeps backed by TI can be run in minutes or hours

Conclusions

- Threat hunting is one of the best tools available to organizations in order to stay ahead of adversaries
- You should aim to minimize the space attackers can work where you will not find them
- Don’t wait on a vendor or the FBI to notify you of breaches – be active and find them yourself!

Questions/Comments?

- Contact Information:
  - andrew@dfir.org (0xB2446B45)
  - @attrc

- References

[1] http://seanmason.com/2014/12/09/a-hunting-we-will-go/
[2] http://blog.handlerdiaries.com/?s=hunting&submit=Search
[3] http://2014.video.sector.ca/video/110341603
[4] http://www.hexacorn.com/blog/
[5] https://sysforensics.org/2014/01/know-your-windows-processes.html
[6] https://technet.microsoft.com/en-us/library/cc748841.aspx
[7] http://blog.handlerdiaries.com/?p=437

VOLEXITY