Lessons Learned from the Financial InfoSec Trenches

Alex Cox, MSIA, CISSP, GPEN,GSEC
Former Lead Emerging Threat Analyst
Large Financial Services Company

alex@perpetualsec.com
www.twitter.com/perpetualsec

Don’t trust your vendors to protect you!

- A/V and Content Filtering technologies are behind.
- 24hr+ gap between signature deployment and infection (we’ve seen months!).
- That’s 24hrs+ of data loss!

Develop a basic malware analysis capability!

- Malware is driving the criminal economy. Keyloggers, infostealers and proxy bots abound.
- AV alerts tell you that systems are seeing badness but second stage communication pinpoints infection where no signatures exist. (badguys tend to re-use dropsites during an active campaign)
- Consider specialized malware analysis training for senior incident responders.

Online Tools: VirusTotal, Anubis, Wepawet, JSunpack

Implement a Network Forensics capability!

- Disk Space is cheap, solutions exist that can record *all* traffic to and from the internet at your organization, homegrown and commercial.
- Being able to go “back in time” to see what actually happened is a life saver that can help in many many ways and can tie security event logs together.
- Being able to actually see exploits in action gives you insight into criminal actions and thought process.
- It’s easier to get money for projects from the big wigs by being able to say “This is what is happening.” rather then “This is what could happen.” Ex: RBN

Tools: Wireshark, Tcpdump, NetWitness, Netscout

Think high level!

- High level details can help you identify badness and “focus the funnel”
- Look at ASNs, Registrars, Registrants, filenames, directory names and domain country codes.
- After some time doing this you can use “pre-cog” detection and be proactive (“I’ve seen this ASN before and it’s always been bad, so I’m going to blackhole it” or “This particular filename has been associated with lots of badness in the past, so I’m going to look for it”).

Tools: Robtex, Team Cymru, mynetwatchman, SANS

Research is Key!

- Review as many data sources as you can to paint pictures and direct research. AV "can't clean" logs are great, but AV "cleaned just fine" are even better! Same with content filtering blocks.
- Get tied into the research community...lots of great resources and minds online.
- Don't be afraid to reach out to researchers if there is a need. Ex: Dan Kaminsky was a great help during our response to his DNS caching vulnerability (CheckFree compromise).
- Don’t forget to watch your own gates!

Tools: RSS Feeds, Twitter, company research blogs, news

?