What Will You Investigate Today?
$ whoami

- Xavier Mertens (@xme)
- Consultant @ day
- Blogger @ night
- BruCON co-organizer
“The opinions expressed in this presentation are those of the speaker and do not necessarily reflect those of past, present employers, partners or customers.”
Agenda

• Introduction
• Interesting protocols
• Public resources
• Toolbox
Feeling This?
Me? Breached?

• In 66% of investigated incidents, detection was a matter of **months** or even more

• 69% of data breaches are discovered by **third** parties

(Source: Verizon DBIR 2012)
“Grepping” for Gold

- Tracking users
- Suspicious traffic
- Out-of-business
- Compliance
- Exfiltration
- “Below the radar”
Sources

- OS / Applications Events
- Network protection (FW, ID(P)S, Proxies, etc)
- Users Credentials
- IP, Domains, URLs
- Digests (MD5, SHA1)
- Metadata
Multiple Sources

- Automatic (logfiles, events)
- Online repositories
- Internal resources
- Developers!
“Active” Lists

- Temporary or suspicious information to track and dynamically updated

- Examples:
  Contractors, Admins, Terminated Accounts, Countries (GeoIP)

- If grep(/$USER/, @ADMINS) { ... }
Correlation

Your Recipes

Evidences

Local Data
Public Data
Generated Data
Visibility!
Agenda

- Introduction
- Interesting protocols
- Public resources
- Toolbox
DNS

- No DNS, no Internet!
- Can help to detect data exfiltration, communications with C&C (malwares)
- Alert on any traffic to untrusted DNS
- Allow only local DNS as resolvers
- Investigate for suspicious domains
HTTP

• HTTP is the new TCP
• Investigate for suspicious domains
• Inspect HTTPS (Check with your legal dept!)
• Search for interesting hashes
SMTP

- Track outgoing emails
- Investigate for suspicious domains
Netflow

- Analyze network flows
- Src Port
- Src IP
- Dst Port
- Dst IP
- Timestamp
Agenda

• Introduction
• Interesting protocols
• Public resources
• Toolbox
IP Addresses

- Correlate your firewall logs
- GeoIP
Domains

• DNS-BH (malwaredomains.com)
  http://mirror1.malwaredomains.com/files/domains.txt
  http://mirror1.malwaredomains.com/files/spywaredomains.zones
  http://www.malwaredomainlist.com/hostslist/hosts.txt

• Correlate your resolver logs
URLs

• http://malwareurls.joxeankoret.com/normal.txt

• Google SafeBrowsing

use Net::Google::SafeBrowsing2;
use Net::Google::SafeBrowsing2::Sqlite;
my $gsb = Net::Google::SafeBrowsing2->new(
  key => "xxx",
  storage => Net::Google::SafeBrowsing2::Sqlite->new(file => "google.db")
);
$gsb->update();
my $match = $gsb->lookup(url => "http://evil.com");
if ($match eq MALWARE) { ... }
“Data are provided for ‘free’ but the right to us can be restricted to specific conditions (ex: cannot be re-used for commercial applications). Always read carefull the terms of use. Some services require prior registration and use of APIs”
OSINT

“Set of techniques to conduct regular reviews and/or continuous monitoring over multiple sources, including search engines, social networks, blogs, comments, underground forums, blacklists/whitelists and so on. “
OSINT

• Think “out of the box”!
• What identify you on the Internet?
  • Domain names
  • IP addresses
  • Brand
Agenda

• Introduction
• Interesting protocols
• Public resources
• Toolbox
pastebin.com

- A gold mine for exfiltrated data!
- Tool: pastemon.pl
- https://github.com/xme/pastemon
Data Parsers

- d3.js Javascript library
- Example of implementation: malcom (Malware Communications Analyzer)
- https://github.com/tomchop/malcom
Data Parser
The Conductor

- OSSEC
- Log Management
- Active-Response
- Powerful alerts engine
Online Tools

- http://urlquery.net
- http://www.scumware.org/index.scumware
- http://bgpranking.circl.lu/
- https://malwr.com/
- http://www.informatica64.com/foca.aspx
- http://virustotal.com
Conclusions

• Know your environment
• You have plenty of useful (big)data
• Free software can help you (but the project is not free)
Questions?
@xme
xavier@rootshell.be
http://blog.rootshell.be
https://www.truesec.be