Maltego Tungsten as a collaborative attack platform

BlackHat 2013
About us
Schedule

• Why did we do this?
• Introduction to Maltego Tungsten
• Maltego with Teeth
  – Design principles
  – Infrastructure attacks
  – Attacking people
  – Attacking mobile devices
Why did we do this?

- Maltego Tungsten is our airframe
- The plan is to provide a platform that can
  - Visualize complex information
  - Allows humans to spot patterns
  - Share it
    - Anonymously
    - In real time
  - Run actions on entities
    - Based on value, position in graph
    - Actions could be *anything*
- This is our day job. But we want to show how it can work
  - We built some ‘demo’ weapons
  - You should really be building it...
Introducing Maltego Tungsten

• Two main features:
  – Collaboration
  – Undo/redo

• Collaboration (comms) design principles:
  – Uses XMPP
  – Can use public infrastructure (e.g. not Paterva)
  – Encrypted on message layer with symmetric key
  – Aliases separate to XMPP username – anonymous, lack of attribution.
Maltego Tungsten

- Sync entire graph, notes, bookmarks etc.
  - Does not sync attachments (yet!)
- Syncs layout, not viewport
- Also chat window / status
- Can run transforms / machines

- To join investigation you need to know:
  - The investigation name
  - The key
  - The server (XMPP) used
Tungsten demo
MaltegoTeeth - Intro

- We wanted to build an attack platform with the following in mind
  - Multiple attackers can work together
  - Large network (think nationwide or multi national)
    - Find the vulnerable host, not the vulnerability on a host
  - No 0 day
    - That’s cheating!
  - External, over the Internet
  - Black box, zero knowledge
MaltegoTeeth - Intro

• Free!
• Runs on Kali Linux
  – Known platform with goodies pre installed
  – We don’t need to re-invent the wheel
• Using local transforms
  – Real time logging, status reports
  – Runs off the local machine, portable.
• Open source easy to read Python code
  – Code is REALLY simple
  – You are welcome to improve, change
  – We’re not coders so it’s hackish.
    • But we like it like that!
Main areas of interest

• Infrastructure
  – Everyone here knows this space pretty well
  – Mainly web servers, SMTP servers, FTP and the odd open port

• People
  – Semi automatic social engineering with real tangible results.
  – “Spear turret”?

• Personal computing devices
  – PCs
  – But mostly mobile devices
    • Phones
    • Tablet
Machines
... not people
Infrastructure - Foot printing

• Most people think Maltego is great for profiling people.
• Maltego is even better at working with structured data.
• Maltego is very strong in footprinting
  – Radium machines - L3 footprint
Maltego footprint demo

• Examples of footprints already done:
  – Pentagon
  – AEOI
  – CIA
  – XXX government (partial)

• Let’s do it live
  – Pick a target from Fortune 1000
Infrastructure

• What can we get from it?
  – Besides good target selection
• We’re probably dealing with
  – Web servers (HTTP/HTTPS)
  – SMTP servers
  – FTP/VPN
  – Odd 3389, 22, 23 (perhaps)
What can we get from web servers?

• Remember – no oday!

• File and directory mining
  – Unlinked files / directories / admin backends

• SQL / RFI injection
  – On surface level

• Protected by a single password
  – Content Management System (CMS)
    • Think Wordpress, Joomla, cPanel
  – OWA
  – Web VPN, Citrix, etc.
Directory / File mining

• Not as easy as you’d expect
  – Many scanners do this horribly wrong
  – Need to look at server responses, not HTTP status codes

• Search for
  – Files
    • In known locations / In discovered directories
  – Directories
    • In known locations / In discovered directories

• Get known locations?
  – Crawl / mirror the site
  – Look for sitemap.xml or robots.txt
  – Search engines already crawled it (sometimes)
File / Directory mine demo

- Find directories / files in root
- Find known locations via
  - Sitemap.xml
  - Crawl / mirror
- Find directories / files in known locations

- While you are there
  - Check for indexability of directories
Possible Injection Points (PIPs)

• When we’ve mirrored/crawled site we also know
  – What web forms are on the site
  – URLs with GET parameters
    • Eg /search.php?terms=
• We can decide which forms are interesting:
  – Parameter value
    • Action=print is likely not interesting
  – Parameter name
    • __VIEWSTATE is likely not vulnerable
    • btnSubmit is not interesting
PIP demo

• Crawl a site
• Set up ignore fields and values
• Show PIPs

• Attack PIP
  – Fire SQLMap for every PIP
Possible Entry Points (PEPs) - OWA

- We looked at Fortune 1000. About 60% use OWA without additional security.
- Means username / password gives access to
  - Email
  - Address book, calendar
    - Gold mine for social engineering
- MS username vs. email address
- MS domain vs. email address
- Default domains
- Lock out / denial of service
Possible Entry Points (PEPs)

• OWA is protected by
  – Form based login
    • Mechanize
  – NTLM
    • Hydra

• OWA versions:

• We’re lazy. Built fingerprint matching thingy. Side effect:
  – Also identifies
    • Citrix, Cisco Web VPN, SecureID, RSA and 19 others
PEP (OWA) demo

- Identify OWA interface
  - Look for common names
  - Check open 443
  - 401? NTLM
  - Match fingerprint to list of prints

- Select email addresses
- Run brute force
Possible Entry Points (CMS)

• Joomla / Wordpress / cPanel are mostly on the same spot.
  – Word press – use Metasploit plugin
    • Nice template to work with Metasploit
  – Joomla – used Mechanize and rolled our own
  – cPanel ...
CMS Brute demo

- Find
- Attack...

- That’s really all there is to it.
  – Click, click bang
Vulnerability scanners

• We looked at scanners.
• It felt like this:
Vulnerability scanners

• We settled on Nmap with NSE
  – Free
  – Fast
  – Light
  – Reliable
  • ... kind of
  – Scripts seems to be written by hackers.
    • We like that.
  – Easy to integrate
  – Easily extendable
  – More than 400 scripts with Kali
Vuln scanner

• Depends on the family you using
• Finds all the usual suspects
  – Weak SSH / MySQL / MSSQL / VNC passwords
  – Anonymous FTP
  – PUT HTTP method
  – FrontPage (90s called!)
  – SMTP relay open
  – etc
Demo – Nmap with NSE

• Configure family
  – auth, default, discovery, external, intrusive, malware, safe and vuln, none, all
• Where needed
  – Configure extra parameters
  – Configure ports
• Point
• Click
• Bang
People
...not machines
People - Maltego side

• The plan
  – Mine email address from target domain
  – Mine email address from address book
  – Get more info from Maltego
    • Social network membership
      – Facebook, LinkedIn, Twitter, Flickr
    • Get more info
      – Manually?
  – Automagically do phishing attack
    • web application (KingPhisher)
People - KingPhisher side

- Parse info from the graph
- Select email templates based on info in the graph
- Based on the info collected and template used
  - Find more info:
    - Facebook / Flickr friends / Twitter profile pic
    - Pretty pictures
    - Interests etc.

Populate template with info from Maltego graph
- Send email...
- Set up collectors
KingPhisher Components

1. POST graph

2. After setup, ready send

2. Collector setup

3. Email sent

4. User visits site

5. Monitor campaign

Target

SMTP sender

KP controller
Attacker
Configures mail

Collector

Maltego client
Challenges

• Getting marked as spam / phishing
  – Their HTML email template
    • Redo the HTML completely from scratch
  – DKIM / SPF
    • Use a different email address, but close enough
  – Certain phrases
    • “Facebook”, Facebook’s physical address
    • Outlook and links with IP addresses
  – Real Time Blacklist (RBLs)
    • Split the email composing and sending components
      – PHP hosting site + SMTP
      – Makes it easier to move the endpoint around
Then...when the user clicks on it

- Serve browser 0day
  - Wait.. that’s cheating! You said no oday! OK..
- Collect IP address, user agent
- Redirect user to fake
  - Social network site
  - Corporate webmail / VPN site
- Hope to collect credentials
- Credential re-use:
  - Use on company infrastructure
    - VPN / Webmail
  - Other social networks
  - Profit!
Useful templates

- Facebook (picture tag)
- Twitter (new follower)
- OWA with web forms
- OWA NTLM / Generic BA
  - Serves Basic Auth prompt
  - Collect creds
  - Rinse repeat (we want to collect everything)
  - Forward to real site
How do you manage the campaign?

Maltego!

• Run 3 transforms perpetually in a machine
  – Controller -> Campaign/Email addresses
    • Emails sent to
  – Email address -> UserAgent and IP
    • That clicked
  – Email address -> Creds collected
    • That supplied credentials
Cool other ideas...

... that we did not implement (or perhaps we did?)

• Add to graph sent to KP / AmIThePresident.com:
  – IP ranges
  – Country
  – Time of day
  – User agent

• Use this to filter
  – When your target matches filter
    • Serve oday / phish
  – When Google/MS/Facebook comes visiting
    • serve ‘Hello World’
King Phisher demo
Mobile devices demo
(if there’s time left!)
RELEASE

Maltego Tungsten / Teeth / KingPhisher

• Released today!
• Check website / Twitter for details
  – www.paterva.com
  – @paterva

Questions?