Agenda

• $whoami
• What we are (and aren’t) going to cover
• Shadow Brokers background
• DFIR implications of the dumps
• Closing thoughts
• Question time
$whoami

- SANS Senior Instructor and Course Author
- IANS Faculty; Rally Security Co-Host
- Founder and President of Rendition Infosec
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- Dislikes: those who call themselves “thought leaders,” “crypto bros,” and anyone who needlessly adds blockchain to a software solution
What are we going to cover?

More importantly, what aren’t we going to cover...
What are we going to cover?

• History of the dumps
• Why I think the Shadow Brokers targeted individuals
• Why you as a DFIR professional should be studying these (and other leaks), even if your boss says “no”
• DFIR implications of Shadow Brokers dumps
What aren’t we going to cover?

- Any classified information not already in public
- I won’t confirm that these tools belonged to NSA
- What specifically I did for NSA
- Why I left
- Who I think the Shadow Brokers are
I know I said we weren’t covering this, but…

Who are the Shadow Brokers?

Lots of people believe they are Russian…

What do I think?
How did they get the tools and data?

• That remains an open question – one that I can’t answer

• Possibilities:
  – Insider threats are obviously possible
  – Could be a hack of NSA’s networks
  – Harold Martin?
  – Kaspersky?
Shadow Brokers Background

Turtles all the way down...
Shadow Brokers Leak Timeline

- August 13, 2016 – Firewall tools/exploits
- October 31, 2016 – List of infrastructure servers
- January 2017 – List of Windows exploits, a few tools
- April 5, 2017 – Linux tools and exploits
- April 8, 2017 – Windows exploits (including EternalBlue)
DFIR implications of the dumps

We are at a DFIR conference, aren’t we?!
DFIR Implications – a quick note

• In this section I’m not interested in talking about the specific ways that the Equation Group may have used the tools we’ll discuss

• The purpose is to highlight capabilities that should force us to fundamentally change what we believe to be both in the realm of the possible and the realm of the “reasonably likely”
DFIR Implications

- Threat hunting Equation Group actors
- Disable Auditing
- Event log editing
- Hacking Oracle
- Threat hunting other actors
• What does your logging look like?
• After analyzing these tools, have you looked through historical data for evidence of connections from the IP addresses released?
• What about tool signatures?
  – Filenames
  – Registry keys
  – Service names
  – Netflow?
  – Packet capture???
Disabling Auditing

- Yes, APT attackers can disable event logging, presumably without leaving additional auditing logs

- It does not appear this is a new capability…

```bash
# This script attempts to disable auditing using all known methods.
# Modifications:
# 03/20/01 Created.
```
• We have evidence that APT groups had the capability to surgically manipulate event logs for some time
• Modification is very possible to detect, but requires hunting in the negative space
• Ask “based on what I see here, is something missing that must be here?”
  – e.g. Windows logoff (4634) with no corresponding logon (4624)
What about accessing data in an Oracle DB without a password?

We knew this was possible from SYSTEM level permissions, but didn’t have a concrete example of implementation.

Matt Suiche (who stood me up here) talked about this at Blackhat last year.

No logging, bypasses table/column encryption.

Example XML code:

```
<Option name="open" group="type">
  <Help>Open up Oracle to login without a password</Help>
  <Set data="type" value="2" />
</Option>
```
• Hungarian researchers disclosed earlier this year that a program called “Territorial Dispute” enabled Equation Group to hunt for other nation state actors

• Now their IOCs are your IOCs!
Living in the Shadows of a disclosure

TFW your threat model changes overnight...
Understand Your Threat Model – I Didn’t

• Nothing stays secret forever

• Intelligence community leaks and compromises are rampant

• Before you do “it” think about how that would look if your actions were suddenly on the front page of the New York Times
Understand Your Threat Model – I Didn’t (2)

• I assumed that what I did:
  – Wouldn’t be detected
  – Wouldn’t be attributed to the US if it was detected
  – Wouldn’t be attributed to me if it was attributed to the US

• I’m now convinced none of that is true
When the Shadow Brokers got *really* mad at me in July 2017, I cancelled some overseas engagements.

It’s hard to model the threat of a disclosure while you are in a foreign country.

It’s MUCH harder to understand the threat of a disclosure made privately to a foreign government.
Question Time

Ask whatever you’ve been dying to know…
• This is being recorded, don’t be offended if I don’t answer your question publicly

• There may be more nuance than I’m comfortable explaining on video in the time allowed

Jake Williams
Rendition Infosec
www.rsec.us
@RenditionSec