MINORITY REPORT: A LOOK AT TIMING OF WANNACRY AND TRUMP'S SPILLAGE

CAVEAT: Note well these two points before continuing –

> 1) Check the byline; this is Rayne, NOT Marcy; we may have very different opinions on matters in this post.
>
> 2) This post is SPECULATIVE. If you want an open-and-shut case backed by unimpeachable evidence this is not it. Because it addresses issues which may be classified, there may never be publicly-available evidence.

Moving on…

Like this past week's post on 'The Curious Timing of Flynn Events and Travel Ban EO', I noticed some odd timing and circumstances. Event timing often triggers my suspicions and the unfolding of the WannaCry ransomware attack did just that. WannaCry didn't unfold in a vacuum, either.

Timeline (Italics: Trump spillage)

13-AUG-2016 – Shadow Brokers dumped first Equation Group/NSA tools online

XX-XXX-201X – Date TBD – NSA warned Microsoft about ETERNALBLUE, the exploit which Microsoft identified as MS17-010. It is not clear from report if this warning occurred before/after Trump's inauguration.

XX-FEB-2017 – Computer security firm Avast Software Inc. said the first variant of WannaCry was initially seen in February.

14-MAR-2017 – Microsoft released a patch for vulnerability MS17-010.

14-APR-2017 – Easter weekend – Shadow Brokers dumps Equation Group/NSA tools on the internet for the fifth time, including ETERNALBLUE.

(Oddly, no one noted the convenience to Christian countries celebrating a long holiday weekend; convenient, too, that both western and eastern Orthodox Christian sects observed Easter on the same date this year.)

10-MAY-2017 – White House meeting between Trump, Foreign Minister Sergei Lavrov, and Ambassador Sergey Kislyak. No US media present; Russian media outlet TASS' Washington bureau chief and a photographer were, however.

12-MAY-2017 – ~8:00 a.m. CET – Avast noticed increased activity in WannaCry detections.

[graphic: Countries with greatest WannaCry infection by 15-MAY-2017; image via Avast Software, Inc.]

12-MAY-2017 – 3:24 a.m. EDT/8:24 a.m. BST London/9:24 a.m. CET Madrid/10:24 a.m. MSK Moscow – early reports indicated telecommunications company Telefonica had been attacked by malware. Later reports by Spanish government said, "the attacks did not disrupt the provision of services or network operations…" Telefonica said the attack was "limited to some computers on an internal network and had not affected clients or services."

12-MAY-2017 – 10:00 a.m. CET – WannaCry

“escalated into a massive spreading,” according to Avast.

12-MAY-2017 – timing TBD – Portugal Telecom affected as was UK’s National Health Service (NHS). “(N)o services were impacted,” according to Portugal Telecom’s spokesperson. A Russian telecom firm was affected as well, along with the Russian interior ministry.

12-MAY-2017 – ~6:23 p.m. BST – Infosec technologist MalwareTechBlog ‘sinkholes’ a URL to which WannaCry points during execution. The infection stops spreading after the underlying domain is registered.

13-MAY-2017 – Infosec specialist MalwareTechBlog posts a tick-tock and explainer outlining his approach to shutting down WannaCry the previous evening

15-MAY-2017 – ~5:00 p.m. EDT – Washington Post reported Trump disclosed classified “code worded” intelligence to Lavrov and Kislyak during his meeting the previous Wednesday.

16-MAY-2017 – National Security Adviser H. R. McMaster said “I wanted to make clear to everybody that the president in no way compromised any sources or methods in the course of this conversation” with Lavrov and Kislyak. But McMaster did not say information apart from sources or methods had been passed on; he did share that “‘the president wasn’t even aware of where this information came from’ and had not been briefed on the source.”

The information Trump passed on spontaneously with the Russian officials was related to laptop bomb threats originating from a specific city inside ISIS-held territory. The city was not named by media though it was mentioned by Trump.

16-MAY-2017 – Media outlets reported Israel was the ally whose classified intelligence was shared by Trump.

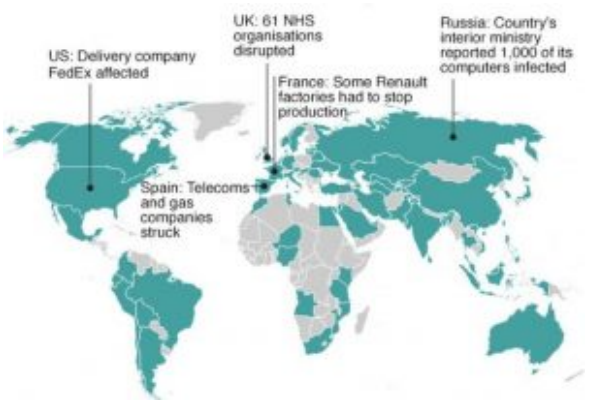
Attack attribution

You’ll recall I was a skeptic about North Korea

as the source of the Sony hack. There could be classified information cinching the link, but I don't have access to it. I remain skeptical since Sony Group's entities leaked like sieves for years.

I'm now skeptical about the identity of the hacker(s) behind WannaCry ransomware this past week.

At first it looked like Russia given Cyrillic character content within the malware. But this map didn't make any sense. Why would a Russian hacker damage their own country most heavily?



[graphic: WannaCry distribution; image via BBC]

The accusations have changed over time. North Korea has been blamed as well as the Lazarus Group. Convenient, given the missile test this past week which appeared focused on rattling Russia while President Putin was attending a conference in China. And some of the details could be attributed to North Korea.

But why did the ransomware first spread in Spain through telecom Telefonica? Why did it spread to the UK so quickly?

This didn't add up if North Korea is the origin.

Later reports said the first infections happened in western Asia; the affected countries still don't make sense if North Korea is the

perpetrator, and/or China was their main target.

Malware capability

Given the timing of the ransomware's launch and the other events also unfolding concurrently — events we only learned about last evening — here's what I want to know:

Can vulnerability MS17-010, on which WannaCry was based, be used as a remote switch?

Think about the kind and size of laptops still running Windows XP and Windows 8, the operating systems Microsoft had not patched for the Server Message Block 1.0 (SMBv1) vulnerability. They're not the slim devices on which Windows 10 runs; they're heavier, more often have hard disk drives (HDDs) and bulkier batteries. I won't go into details, but these older technologies could be replaced by trimmer technologies, leaving ample room inside the laptop case — room that would allow an older laptop to host other resources.

Let's assume SMBv1 could be used to push software; this isn't much of an assumption since this is what WannaCry does. Let's assume the software looks for specific criteria and takes action or shuts down depending on what it finds. And again, it's not much of an assumption based on WannaCry and the tool set Shadow Brokers have released to date.

Let's assume that the software pushed via SMBv1 finds the right criteria in place and triggers a detonation.

Yes. A trigger. Not unlike Stuxnet in a way, though Stuxnet only injected randomness into a system. Nowhere near as complicated as WannaCry, either.

Imagine an old bulky laptop running Windows XP, kitted out internally as an IED, triggered by a malware worm. Imagine several in a cluster on the same local network.

Is this a realistic possibility? I suspect it is based on U.S. insistence that a thinly-justified

laptop ban on airplanes is necessary.

Revisit timing

Now you may grasp why the timing of events this past week gave me pause, combined with the details of location and technology.

The intelligence Trump spilled to Lavrov and Kislyak had been linked to the nebulous laptop threat we've heard so much about for months — predating the inauguration. Some outlets have said the threat was "tablets and laptops" or "electronic devices" carried by passengers onto planes, but this may have been cover for a more specific threat. (It's possible the MS17-010 has other counterparts not yet known to public so non-laptop threats can't be ruled out entirely.)

The nature of the threat may also offer hints at why an ally's assets were embedded in a particular location. I'll leave it to you to figure this out on your own; this post has already spelled out enough possibilities.

Trump spilled, the operation must be rolled up, but the roll up also must include closing backdoors along the way to prevent damage if the threat has been set in motion by Trump's ham-handed spillage.

Which for me raises these questions:

> 1) Was Shadow Brokers the force behind WannaCry — not just some hacker(s) — and not just the leaking of the underlying vulnerability?
>
> 2) Was WannaCry launched in order to force telecoms and enterprise networks, device owners, and Microsoft to patch this particular vulnerability immediately due to a classified 'clear and present danger'?
>
> 3) Was WannaCry launched to prevent unpatched MS17-010 from being used to distribute either a malware-as-trigger, or to retaliate against Russia — or both? The map above shows a disproportionate level of impact suggesting Russia was a potential

target if secondary to the operation's aim. Or perhaps Russia screwed itself with the intelligence entities behind Shadow Brokers, resulting in a lack of advance notice before WannaCry was unleashed?

4) Was WannaCry launched a month after the Shadow Brokers' dump because there were *other* increasing threats to the covert operation to stop the threat?

5) Are Shadow Brokers really SHADOW BROKERS – a program of discrete roll-up operations? Is Equation Group really EQUATION GROUP – a program of discrete cyber defense operations united by a pile of cyber tools? Are their interactions more like red and blue teams?

6) Is China's response to WannaCry – implying it was North Korea but avoiding directly blaming them – really cover for the operation which serves their own (and Microsoft's) interests?

The pittance WannaCry's progenitor raised in ransom so far and the difficulty in liquidating the proceeds suggests the ransomware wasn't done for the money. Who or what could produce a snappy looking ransomware project and not really give a rat's butt about the ransom?

While Microsoft complains about the NSA's vulnerability hording, they don't have much to complain about. WannaCry will force many users off older unsupported operating systems like XP, Win 7 and 8, and Windows Server 2003 in a way nothing else has done to date.

[graphic: 5-year chart, MSFT performance via Google Finance]

Mother's Day 'gift'?

I confess I wrestled with writing this; I don't

want to set in motion even more ridiculous security measures that don’t work simply because a software company couldn’t see their software product had an inherent risk, and at least one government felt the value of that risk as a tool was worth hiding for years. It’s against what I believe in — less security apparatus and surveillance, more common sense. But if a middle-aged suburban mom in flyover country can line up all these ducks and figure out how it works, I could’t just let it go, either.

Especially when I figured out the technical methodology behind a credible threat on Mother’s Day. Don’t disrespect the moms.