The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Putin Hates You? Then Put Less Data Online (Op-ed)

Good old paper-based and oral communication works fine and requires much more effort to spy on.

By Leonid Bershidsky

August 21, 2018

Kremlin.ru

Microsoft Corp.'s announcement that it has taken down a number of fake domains set up by the same cyber-espionage group that allegedly hacked the Democratic National Committee in 2016 shows Russia's interest in U.S. politics isn't ebbing. More importantly, it highlights that the methods these malicious actors have been using since well before the 2016 U.S. election can still be effective.

In a blog post signed by Microsoft President Brad Smith, the company said it had obtained a court order to take over six internet domains set up by "a group widely associated with the Russian government and known as Strontium, or alternatively Fancy Bear or APT28." That's

the group described in a recent indictment obtained by Special Counsel Robert Mueller as consisting of Russian military intelligence officers.

The domains, according to Microsoft, were used in a spear phishing campaign targeting two Republican think tanks, the International Republican Institute and Hudson Institute, as well as the U.S. Senate. Microsoft said it had taken down 84 Strontium-linked websites in the last two years. The software-maker's knowledge of the hackers' operating mode goes back even further: It was described in a company report in November, 2015.

Related article: Russian Effort to Hack U.S. Conservative Groups Thwarted, Microsoft Says

The document detailed two phases of a typical Strontium operation. First, employees of an organization of interest are bombarded with emails, purportedly from a software provider such as Microsoft or Google, warning of an unauthorized attempt to log into an account and providing a link to change a password. Those lead users to fake websites like the ones Microsoft has taken down.

Even if the targets don't swallow the bait and enter their credentials, the impostor site harvests data about their browser, extensions used, computer's IP address, operating system and other particulars by which we're tracked across the internet. These data can then be used to launch other attacks, from more targeted spear phishing emails to attacks based on vulnerabilities in specific software.

Some of these weaknesses have already been fixed, but the attackers know that far from everyone installs security patches as soon as they are issued. Others are "zero-days" – vulnerabilities as yet unknown to software companies.

The Mueller indictment says the Russian intelligence officers were successful in harvesting the login credentials of some DNC employees. Even if they had been less credulous, their computers could have been hacked using vulnerabilities in the software they use.

If there's anything more naive than entering your email password into a phishing website, it's believing that spies, Russian and otherwise, will stop hacking into U.S. political operators' and think-tankers' computers just because of a hullabaloo about an attack on American democracy, an indictment or two and a threat of economic sanctions. Knowing what the adversary is thinking and planning will still be important no matter how many times spies get caught and what potential repercussions follow, short of nuclear war.

Related article: Jailed Russian Hacker Confesses to DNC Hack

In the particular cases described in Smith's post, a Russian interest would be understandable. The IRI counts prominent Russia hawks such as Senators John McCain, Lindsey Graham and Marco Rubio among its board members. The Hudson Institute's top Russia expert is veteran journalist David Satter, banned from the country in 2014, when he was working as a consultant to Radio Liberty.

If Mueller is right about APT28 hackers holding military rank, this is the intelligence service known by its old name, the GRU, doing research on Russia's perceived enemies. Party affiliation doesn't matter for such an effort; any U.S. political operator or expert voicing what the regime in Moscow sees as anti-Russian views is likely to be targeted.

In a way, the Trump-Russia scandal has expanded the spies' area of interest because so many U.S. politicians who formerly showed little interest in Russia have now weighed in. Russian intelligence's interest won't wane after this year's midterm campaign is over; the line between intelligence-gathering and election meddling through the release of compromising information is thin.

That's what makes it especially alarming that methods from 2015 are still in use. After years of being told repeatedly not to click on any email links without knowing exactly where they lead, many in the U.S. political community will still do so.

Microsoft's answer is a service called Microsoft AccountGuard, which provides cybersecurity to "organizations that underprin democracy."

None of this, however, will thwart the occasional click on a malicious link, much less a zero-day attack. What will is a technique used by Emmanuel Macron's campaign during the 2017 French presidential election: his team simply refrained from putting sensitive information on email or online.

Good old paper-based and oral communication works fine and requires much more effort to spy on. When Macron's campaign was, inevitably, hacked, the thieves didn't find anything politically useful or important about Macron or his team.

For those the Russian regime considers hostile, a little old-fashioned paperwork will be key to maintaining privacy.

Leonid Bershidsky is a Bloomberg Opinion columnist covering European politics and business. He was the founding editor of the Russian business daily Vedomosti and founded the opinion website Slon.ru. The views and opinions expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2018/08/21/putin-hates-you-then-put-less-data-online-op-ed-a62604