*** 北米連携センター定期報告***

2014 年 9 月 23 日

●ハニーポット使った重要インフラへのサイバー攻撃調査、米国が最大の攻撃発信元に

【Bloomberg, 2014/09/23】
　電力網、水道、製造工場などの産業制御システムに対するサイバー攻撃は増加の一途を辿っているが、グーグル・ベンチャーズも出資するセキュリティ会社、スレットストリームの創設者で同社 CTO を務めるグレッグ・マーティン氏とブルームバーグのジョーダン・ロバートソン氏はこのような重要インフラに対するサイバー攻撃を分析するための「ハニーポット」を構築。
　産業制御システムに偽装したハニーポットは世界各国で重要インフラがサイバー攻撃にさらされていることを確かめるため、米国、英国、アムステルダム、東京、シンガポールにあるよう見せかけられ、先週までの 3 ヶ月間、サイバー攻撃の拠点などが分析された。
　その結果、攻撃トラフィックが最も多く発信されたのは米国（6000 件以上）で、以下、中国（3500 件以上）、ロシア（2500 件以上）、オランダ、フランスと続いた。
　このような攻撃トラフィックは真の攻撃拠点をくらますためにボットとなったコンピュータを介して行われることも多いが、マーティン氏によると今回のデータは概ねネットワークの脆弱性を偵察するトラフィックを反映しており、このようなデータは真の IP アドレスや国を露呈することも多いという。
　また分析結果は米国が攻撃の真の拠点ではなかったとしても攻撃トラフィックを仲介する大きな経路になっていることを示すものだとしている。
　さらに同氏は脆弱性を偵察するデータの一部がセキュリティ会社や学術機関のものである可能性はあるが、大きな部分は軍事機関によるものが占めると見ている。

（参考）本件報道記事
A Decoy Computer Was Set Up Online. See Which Countries Attacked It the Most

By Jordan Robertson - Sep 23, 2014

If you build it, they will come. And attack.

Earlier this year, I was brainstorming with Greg Martin, the founder and chief

technical officer of ThreatStream, a Google Ventures-backed security startup, about finding a way to show the global nature of attacks against industrial-control systems used in electrical grids, water systems and manufacturing plants. For obvious reasons, attacks against critical infrastructure are among the biggest concerns in cyber-security.

Industrial networks are already under daily assault by hackers, and that threat is only growing as more countries develop advanced cyber-war capabilities. Few have been as thoroughly revealed to the public as the United States' through the disclosures of former National Security Agency contractor Edward Snowden.

Martin and I decided on setting up an online decoy known as a honeypot, which was made to look like an enticing industrial-control computer to hackers. It's designed to attract attacks so they can be traced and studied.

The graphic below shows which countries were the apparent source of the majority of attacks.

The fake control systems were made to look like they were located in the U.S., the U.K., Amsterdam, Brazil, Tokyo and Singapore. We wanted a variety of locations to show that systems everywhere are under attack. Over a three-month period ending last week, the U.S. was by far the biggest source of attack traffic (more than 6,000 attacks), followed by China (more than 3,500), Russia (more than 2,500), the Netherlands and France.

The presence of countries such as the Netherlands and France isn't surprising because they are home to well-known hacking efforts, both commercial and state-sponsored, Martin said.

One challenge with a study like this, and a challenge of defending networks in general, is that hackers often route their traffic through infected personal computers called "bots," or proxies, which disguise their true location. So, some of the computers were likely used without their owners' knowledge, with the hackers residing in other countries.

That said, the data largely reflect reconnaissance missions, in which hackers

often use less obfuscation, Martin said. These probes to learn about networks don't set off the same alarms that attempts to break into the targets do, so reconnaissance data can reveal many true IP addresses and countries of origin. Nation-states also sometimes launch attacks from bots within their own borders because the government controls the Internet providers, he said. More than anything, the experiment shows that the U.S. is the conduit for a lot of the world's attack traffic, even if it's not the source of all of it. And a lot of other countries have their hands in the honeypot as well, as nation-states and private firms race to find the latest vulnerabilities in critical infrastructure.

"It's not unlikely that some probes are from security companies and academia, but the dataset is large and diverse enough that it probably includes a large amount of military organizations, if not all of them (proxied or not)," Martin wrote in an e-mail.

The honeypot idea was inspired by work that Kyle Wilhoit, a threat researcher at the security firm FireEye, previously did where he replicated the network of a municipal water system that looked like it was in Ashburn, Virginia, population 44,000. The virtual utility was raided within weeks by what Wilhoit said he believes was a Chinese military hacking unit, which stole passwords, engineering PDFs and other data. A later version of the experiment saw hackers, most of them in China, override controls in fake water plants in Europe and Asia.

Source :
http://www.bloomberg.com/news/2014-09-23/a-decoy-computer-was-set-up-online-see-which-countries-attacked-it-the-most.html

以　上