Related news

cyberscoop.com/ukrainian-cyber-attacks-russia-conflict-q-and-a/

January 31, 2022

geopolitics

Conversation with a top Ukrainian cyber official: What we know, what we don't, what it means

The Ukrainian national flag flies during a public celebration for the 30th anniversary of Ukrainian independence, on Aug. 24, 2021 in Lviv, Ukraine. (Photo by Adam Berry/Getty Images)

Written by AJ Vicens

Jan 31, 2022 | CYBERSCOOP

Cybersecurity officials in Ukraine issued a warning Monday about yet another phishing attack using either compromised or spoofed government email addresses, the second such warning since Saturday.

Monday’s alert warned of attackers targeting government institutions with malware-laced bait documents hosted on Discord that come to targets within emails from the National Health Service of Ukraine. The malware deploys a program called OutSteel that looks for certain file extensions and steals them, and also deploys a second malicious program called SaintBot.

Monday’s bulletin comes two days after government officials there warned of compromised email accounts from the Ukrainian judiciary being used to target mostly Ukrainian government targets with malware hidden within phony court inquiries.

Both operations come roughly two weeks after a cyberattack targeting Ukrainian government systems that wiped some computers and defaced the websites of dozens of agencies’ sites.

All of the attacks are linked as part of “hybrid aggression, cyber aggression against Ukraine,” said Victor Zhora, the deputy chairman of the State Service of Special Communications and Information Protection of Ukraine, but not as a single operation.

“These are steps to continuously attack Ukrainian government agencies, objects of critical infrastructure and to make us ready for any kind of new attack,” Zhora said.

The operations play out against the backdrop of ongoing tension between the government of Russia and a host of western governments, as the Russian government accused the U.S. of wanting war in Ukraine, and the U.S. continuing to insist that a Russian military attack on Ukraine is possible at any time.

As the two nations’ diplomats traded barbs at the United Nations Monday, officials in Kyiv such as Zhora are tasked with unpacking the technical details, as well as the methods and motivations, behind ongoing cyberattacks directed at the government Ukraine.

Zhora spoke with CyberScoop Monday and explained the biggest outstanding questions related to the cyberattacks against his country, how the attacks fit into the context of Russian aggression toward Ukraine for the last eight years, and how other countries, including the U.S., are helping decipher what’s happening in the attacks. The answers have been lightly edited and condensed for clarity.

CyberScoop: A fair amount of data and context has been published about the latest round of cyberattacks on Ukraine. What are the biggest unanswered questions?

Zhora: I would name two major questions. The first is the exact way and date of the compromising of the infrastructure software development company, which was used as a first step of a supply chain attack on government websites. That’s what we need to discover.

And that would be a key to the second major question: Attribution. We see a lot of signs, and a lot of details, which can lead up to the conclusion that one of the Russian (advanced persistent threat) APT groups are responsible for this attack, but we need exact proof, which can allow us to come out with a solid attribution.

CyberScoop: There have been public accusations of Russian-government involvement, but you're saying that you want to be able to provide more forensic and digital evidence before formally attributing the attacks to specific groups?

Zhora: We should have enough evidence before we blame anyone responsible for organizing an attack. We already invited [experts] — and hopefully, we'll be able to come out with — a single statement involving international experts who will enrich our expertise.

CyberScoop: There have been reports of U.S. and other nations' cybersecurity experts aiding Ukraine. What does help look like?

Zhora: We appreciate the help from U.S. companies and officials, that is very valuable for us. We have had some talks with different people, and we feel the support and practical support. We continue getting valuable information, which allows us to continue investigation.

As regards to some experts who will help in investigation, unfortunately, I cannot name them or their organization, but I'm confident their help will be very important and valuable for us.

CyberScoop: I would imagine your local experts are quite experienced with dealing with the kinds of attacks they're seeing.

Zhora: Providing comprehensive attribution means not just collecting evidence but also making some conclusions from this evidence. It also should be combined with some intel data and this intel data is particularly rich and fully owned by our foreign partners.

So I cannot say that Ukraine can provide such deep threat intelligence or APT intelligence like the United States or United Kingdom can help with. That's an area of cooperation to provide us solid attribution. And that would be important, that this attribution should convince everybody that all steps that were taken were correct.

CyberScoop: There have been reports of possible Belarusian connections to some of the cyber activity that has been witnessed. Can you elaborate on any of that?

Zhora: That was one of the questions, and could be one of the versions [of events]. For example the [attack] could be developed in the Russian Federation but executed by Belarusians. Or the territory from which Ukraine was attacked could be a territory of Belarus, and that could be done during the military exercises, which took place exactly at the same time. But in my opinion, I don't think that Belarusians would take the risk of being blamed for this.

We understand that we have Russian troops, Russian soldiers, Russian arms, at the east, that have occupied and annexed Crimea. We understand that this is [Vladimir] Putin, this is the Kremlin, this is the Russian Federation. But with regards to Belarus, they always try to keep their neutral position. And if it happens that they were somehow involved in this, that would significantly change the total disposition of forces and there could be some geopolitical changes with regards to this effect. So as an idea, it can exist, but as facts, I don't think so.

CyberScoop: Ukrainian President Volodymyr Zelensky has said Western governments are inciting "panic" by insisting that the Russian government will launch a full-scale attack any day. Do you think that includes any of the discussion around the cyberattacks that are making the headlines?

Zhora: We consider this as a part of this hybrid aggression, parts of a big-information, psychological special operation against Ukraine. Of course, we see the big geopolitical tension and some speculation about a potential land operation. In my opinion Kyiv is rather calm and people are thinking about their day-to-day problems and about dealing with COVID-19, and so the same things people are dealing with around the world. So that's a much more important problem.

But of course, I understand that I cannot see the whole picture as the foreign leaders can see. So my picture is about cybersecurity, and I will say that it's not scary, but alarming. We witnessed the recent cyberattack which shows us some serious weaknesses, which we need to quickly resolve. And the latest phishing campaigns confirm the adversary's abilities and their will to to continue aggression.

This means that critical infrastructure should be our main point of interest. We need to be aware of risks that can happen to critical infrastructure, especially regarding this winter time and potential energy prices, which is basically coming for the whole world.

CyberScoop: Cisco's Talos threat intelligence unit recently warned companies with connections to Ukraine to treat the cyberattacks seriously, but also to avoid "panic" and that cybersecurity experts have seen these kinds of attacks in Ukraine "on and off for years." Is the activity we're seeing in recent weeks evidence of more attacks than usual, or is the quantity of attacks relatively stable?

Zhora: The growth is constant. So each month, we register up to 10% growth of attempts. So it's normal way of things, and that's the situation that we need to to understand and to try to live with.

Just the same way as we live with constant shooting on the eastern border. It's absolutely quiet here in Kyiv and 99% of Ukrainian territory, but unfortunately, almost every day or week, we have victims from Ukrainian troops on the east. That's a situation which has lasted for eight years, and nobody knows how many years it will last more.