Heather (00:05):

Welcome to the Hurricane Labs podcast. I'm Heather. And today we're going to talk about the cybersecurity issues related to the Russia-Ukraine conflict. Now, as you are all likely aware, Wednesday evening, Russian forces began their invasion of Ukraine and the physical attacks have been paired with a range of cyber attacks here to help discuss the implications of this conflict for the cybersecurity community, we have our Director of Security Operations, Josh Silvestro, and our director of Splunk Operations, Steve McMaster. Guys, thank you a whole bunch for taking the time on short notice to join me today. I do really appreciate it.

Josh (00:41):

Of course, you're welcome.

Steve (00:42):

Yeah. Happy to be here.

Heather (00:43):

So first things first, what sort of cyber attacks are being reported as being used against Ukraine? What's being seen?

Josh (00:50):

Well, so far everyone's been reporting that it's really been an ongoing malware campaign over the past couple weeks or potentially even months, you know, in short, Russia's been distributing malware that is being referred to as a wiper and wiping data from PCs making them unusable. You know, there's obviously the always common barrage of attacks, things that everyone sees across any, country or organization, but currently the, again, the biggest reported thing is the malware distribution.

Steve (01:19):

And I think something that's important to keep in mind as we talk about this too, is theyou know, any, any attacks that we see especially coming from, from Russia towards Ukraine arethey're gonna be, this is, this is not new for Russia. Russia has clearly been planning this for a while. And so there, there are likely to be a lot of situations where, you know, the, the attack actually started a while and Russia's just going to start taking advantage of, of the, the foothold that they've already built and just kind of kept quiet.

Heather (01:50):

And that's where we're seeing the term dwell time, right? That this malware or, or the compromise is necessary for these attacks have been in place for some time.

Steve (01:58):

Correct. And another thing too, to keep in mind is, is there will also be a lot of misattribution over the, you know, the coming weeks and months of, of attacks that that may affect Ukraine, but they, they also may not actually be part of this part of this wave too. So as we keep talking about that, I think that's important to keep in mind, but I think what the biggest thing we're going to start seeing is you know, higher visibility attacks, higher higher value targets are, are gonna start popping up. And again, those may be things that, that have been compromised for a long time, but, but now is the time to start taking advantage of that foothold,

Heather (02:33):

Like attacking things like critical infrastructure, right? Like they're not just willing nilly attacking random things like they are going after specific things like telecommunications.

Steve (02:41):

Correct. And I think, but the other thing I you know, you're, you're never gonna go directly after critical infrastructure either. So smaller, smaller businesses, smaller targets within Ukraine and, and in other areas too. But for now, you know, especially in Ukraine are gonna be, you know, jumping off points for attacks against critical infrastructure. So, so while, while critical infrastructure is the primary target or one of the primary targets, the, the smaller places are gonna be more like collateral damage as again, as, as jumping off points for those bigger attacks.

Heather (03:14):

So what more specifically are we seeing as far as how they're attacking?

Josh (03:17):

Yeah. So one of the things that's actually really interesting you know, malware's ever evolving and changing and, you know, for the long, long time now feels like forever. Ransomware's been the big thing where they're actually encrypting drives and, and holding your data ransom, or, you know, in this type of situation could even just render your computer useless. But that takes time. What's really interesting is they're using a you know, this malware wiper they're actually using a legitimate software called EaseUs E–A–S–E–U–S partition manager, which anyone that's ever done, any kind of it administration's probably heard of or used. At its core, it's a legitimate software. It's popular. They're actually using that to just wipe a few bites of the master boot record, you know, that's thing that tells windows, for example, how to start and what to do when it starts. So it's very quick and very effective. You're just wiping, I think I'd seen about 500 bytes, which is, you know, smaller than the average photo on your phone and then shutting the computer down. So then when, you know, whoever goes to reboot it or turn it back on it just can't boot, which is, you know, really fast, really effective. You know, there are ways to repair that and fix that, but, you know, in time sensitive situations, such as war time, that's obviously a, a potentially critical situation. If you can't essentially boot your computer to do communications, take actions, coordinate things. The other thing I'd seen as well is that you know, kind of in relation to how long have they been there, or, you know, what have they compromised? I saw that it looks like they'd tied back a intrusion going back a while to a windows domain controller, and then use that to essentially distribute malware throughout the network. You know, if your domain controller is compromised that's kind of every admin sphere, cuz that is where all computers check in. That's where user accounts are created, permissions are set it really controls most of your it actually controls all of your windows domain for the most part. So it looks like that was compromised, which is, is a big win for any hacker. And then use that to kind of push 'em out to key machines.

Heather (05:19):

So as far as us is businesses go, how concerned about cyber attacks? Should we be, and who is currently most likely to be at risk?

Josh (05:28):

That's actually, it's a good question. Anytime, anything even outside of what's going on in Ukraine any big world events happen, you know, obviously everyone's immediately concerned about, are they a target? And right now, I mean, the truth is for the purpose of what Russia's trying to accomplish, Ukraine is the target, but malware tends to some extent do its own thing, right? When, when malware's written, the general purpose is to spread cause damage and keep spreading cause more damage. So at this point doesn't look like any anyone's reporting, seeing any types of that wiper malware really outside of the general Ukraine region, that being said you know, if it starts to spread through other connected networks or they even talked about, you know, if additional troops from other countries kind of came in connected to the network to provide support for Ukraine, it could spread that way. So it's possible at some point that malware wiper kind of works its way back to other parts of the U.S. You know, not necessarily intentionally, but just by the nature of how malware tends to replicate and distribute. That being said typically when these things happen, the biggest corporations you see under attack are, you know, the energy pipeline, stuff like that. Anyone providing core resources to any country would really be the bigger targets cuz something like that could be crippling.

Steve (06:46):

I think in addition to that you know, just like we talked about a minute ago about smaller, smaller value targets in Ukraine there's definitely the potential for smaller value U.S. Business targets as well. Again, just as, as kind of a, a launching off point, but in, in many of those cases, again, I would, I would think that you know, we should keep in mind that some of these compromises could be, could be months or even years old at this point. And they're gonna be taken advantage of now rather than rather than new compromises just as, as again, launching off points to the bigger, bigger targets. But I do think that for the, for the specialized advanced APT kinds of kinds of threats, it is the bigger businesses that are, are more at risk, especially as, you know, as, as the, the, the cyber engagement. So speak moves from, from just targeting Ukraine, to targeting, you know, anybody who stepped in to on the side of Ukraine in the conflict. I would expect to that, you know, that to start spilling over, not just as collateral damage at that point, but as retaliation for the support being shown to Ukraine.

Heather (08:00):

What sort of things are we doing here at hurricane labs and what sort of things can security teams in general do as this situation continues to develop?

Josh (08:09):

Yeah, so currently at this point really the, the best course of action is you know, in relation to the malware dropper or wiper making sure that your products and everything are up to date, you know, checking with your vendors to see what kind of detections or preventions they have in the product already available to help with that. You know, as some additional IoCs or indicators or compromise become public knowledge we regularly add those to our threat lists. So that way, you know, if, if those IoCs are seen in network logs, we can kind of hopefully get an early indicator that something malicious might be happening and then we can alert on it and help our clients take action. The truth is though in these situations, you know, the best defense is a good offense, you know, when we build use cases and get clients implemented within our SOC here we have a variety of use cases that we roll out as best practice things to look for vulnerability scanning pivoting between systemsrepeat failed logins, just trying to look for any potential signs that something malicious is happening in or against your network. And, and truthfully, those are still really a good source of detections. You know, I know it's not specific to seeing something that you can immediately say, oh, that's Russia. But in, in cases where there's advanced APTs and stuff, those can be tricky, but in compromise networks when there's, you know, a review down the road of what exactly happened, you typically see a lot of the same tactics and techniques used which is why here, when we do use cases, we map 'em all back to the MITRE ATTACK framework, just to make sure that, you know, we're, we're mapping to real world use cases and actual threats that have been seen out in the wild.

Steve (09:40):

And I think that's a good point that especially if you are, if you're not one of the, the bigger targets, if you are a smaller, even medium sized business not again, likely to be in the category of a place, that's gonna be a job jumping off point for a bigger attack. I think the best thing you can do is, is really focus on the basics. You know, the, the more, more you're focused on best practice, good hygiene, the, the, the better off you're going to be preventing yourself from being compromised, being used as a launching off point, and also being the target of, of ransomware wiper attacks.

Heather (10:13):

Are there any key resources that you would recommend people check out for more information?

Josh (10:19):

Yeah. so for some additional resources CISA a is always a good reference if you're not, you should get signed up for their newsletters. So you can get up to date information, not just about the Russia-Ukraine attacks, but as things like Log4j and other big cyber attacks are underway, they're really prompt about sending out alerts and kind of keeping everyone up to date on what's happening as well as what to look for. Symantec also had a blog post about the disc wiping attacks that happened right before the Russian invasion as well as we've sent out an advisory. And is anything additional develops or there's additional details we can share. We'll post those on the Hurricane Labs blog.

Heather (10:57):

All right. Well, again, thank you both for taking the time today. I know this was obviously by necessity, super short notice. I appreciate you setting some time aside this morning.

Josh (11:07):

You're welcome. Happy help.

Steve (11:08):

Absolutely.

Heather (11:10):

And that's all for now for more information, do be sure to check out our links. And again, we will be keeping an eye out as things continue to develop, and if we warranted, we will release an update to this series. Until next time, stay safe.