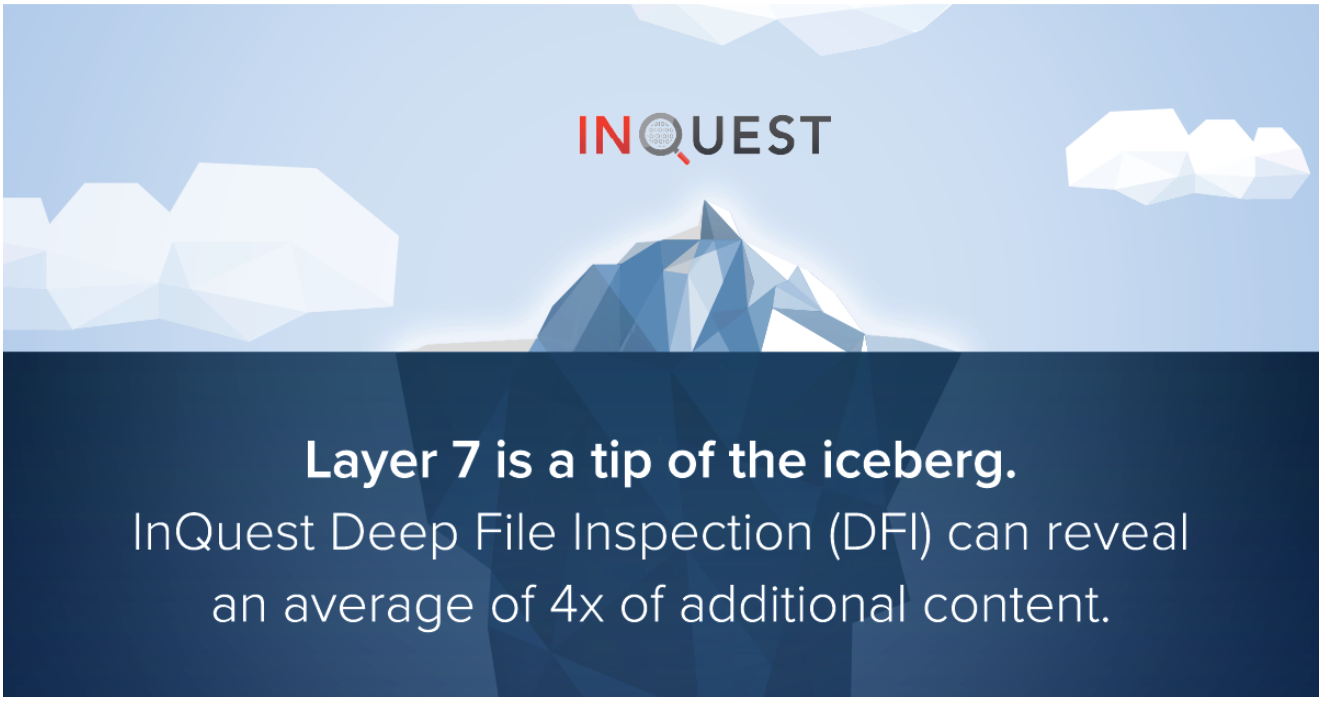
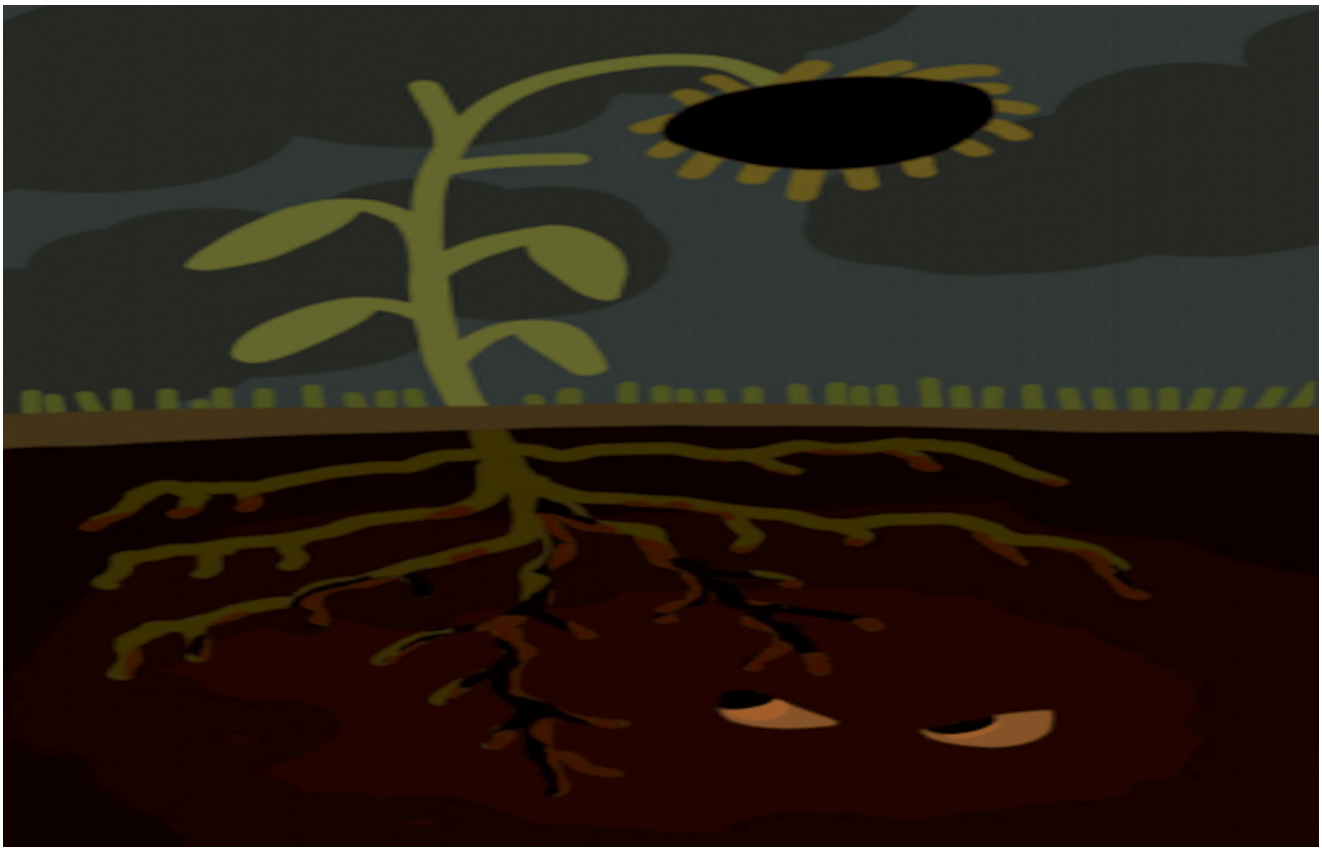
Ukraine CyberWar Overview

inquest.net/blog/2022/04/07/ukraine-cyberwar-overview



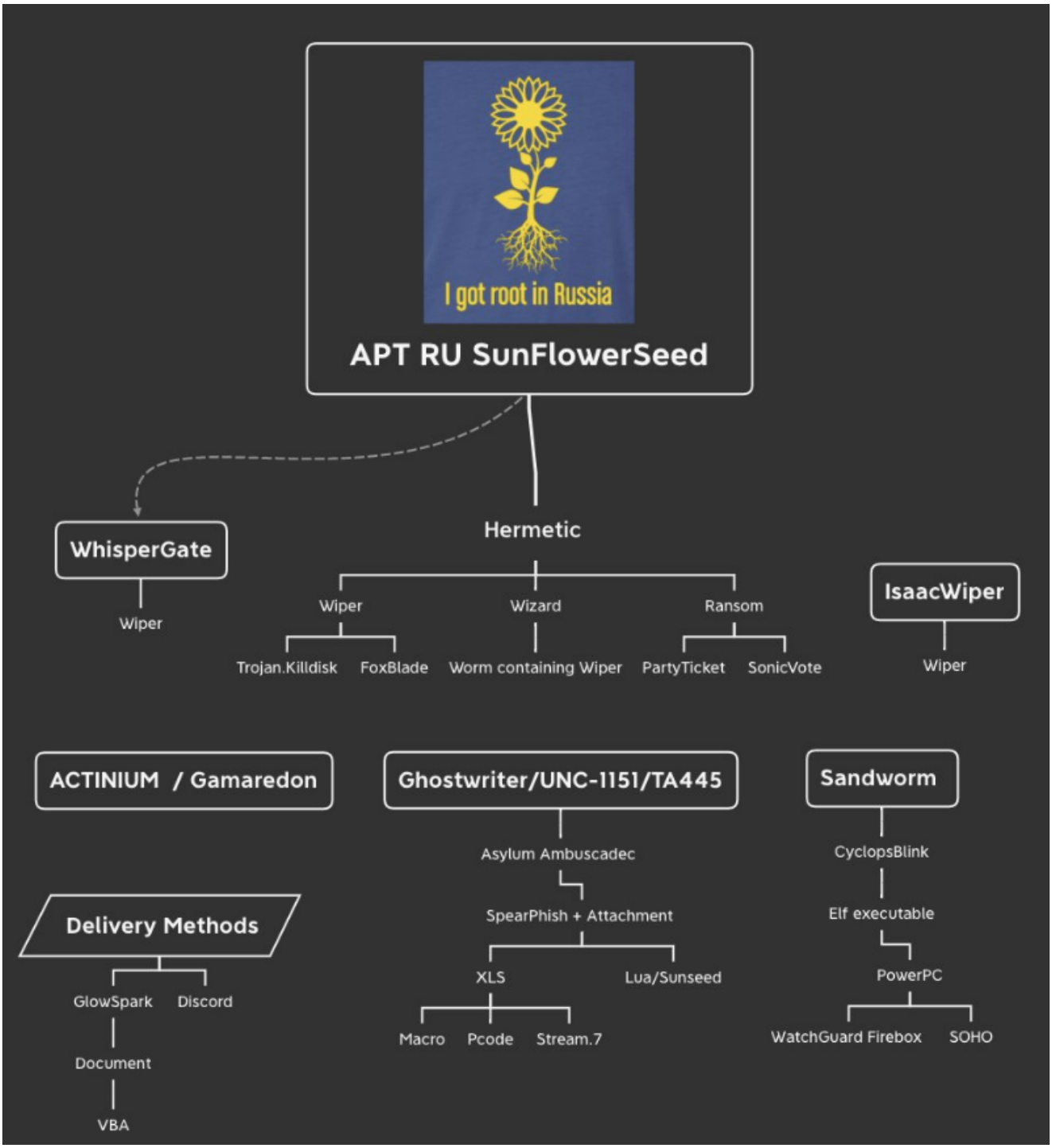


Overview

As the current state of the war against Ukraine has been on everyone's mind for several weeks by now, InQuest Labs has been following activity on the cyber-front proceeding as well as moves made by APTs following the invasion of Ukraine. While the rest of the world is seeing the effects of this escalation with rising fuel prices and supply line hiccups, Ukrainian and Russian citizens alike are clinging onto their livelihoods due to the contempt of Russian leaders. As many within the research community have ties to and/or may be personally affected by this crisis, we felt it was necessary to share any information based on communal efforts that may save lives and contribute to bringing this conflict to a peaceful resolution. Our endeavor with this blog is to document and expose campaigns/associated TTPs as well as provide periodic updates as the situation continues to develop and actors pivot to different tactics. It is imperative that the global effort to contain and reduce the impact of Russian state sponsored threats on the cyber-front does not waver, as further advances could mean innocent lives lost given the current circumstances. Our hope is that the information provided is able to bring those currently engaged in research efforts up to speed along with sparking interest for able minds to join the ranks. True to the message that inspired the name attributed one of the groups that will be covered, video here for the uninitiated (Warning: Language), we are committed to aiding any efforts to stuff as many invading pockets with sunflower seeds as needed to end this senseless war.

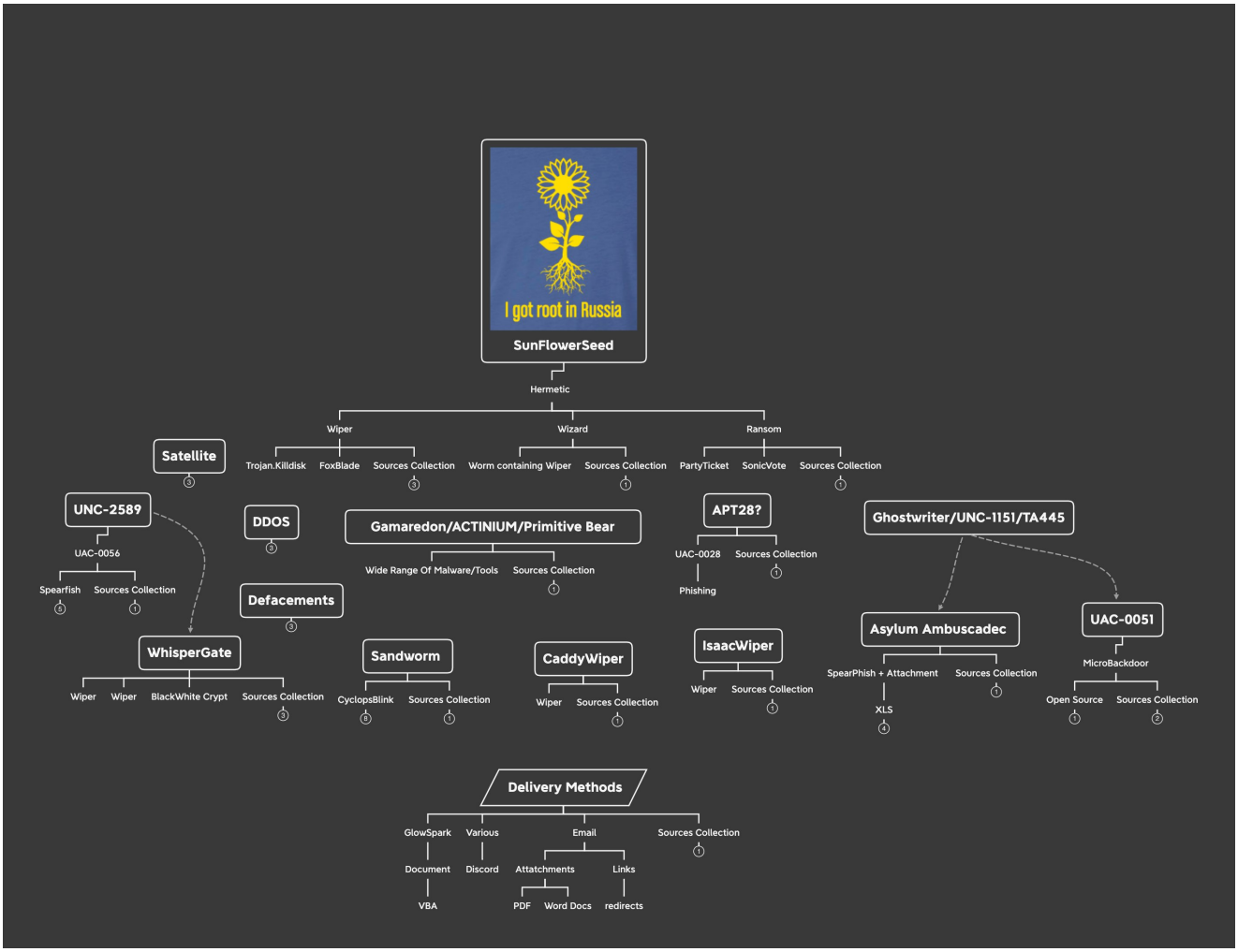
Initially, we published a blog on a delivery mechanism we dubbed GlowSpark, which can be found here.

Next we decided to share an image via tweet that included a high level visual of the threat landscape in an easily digestible format.



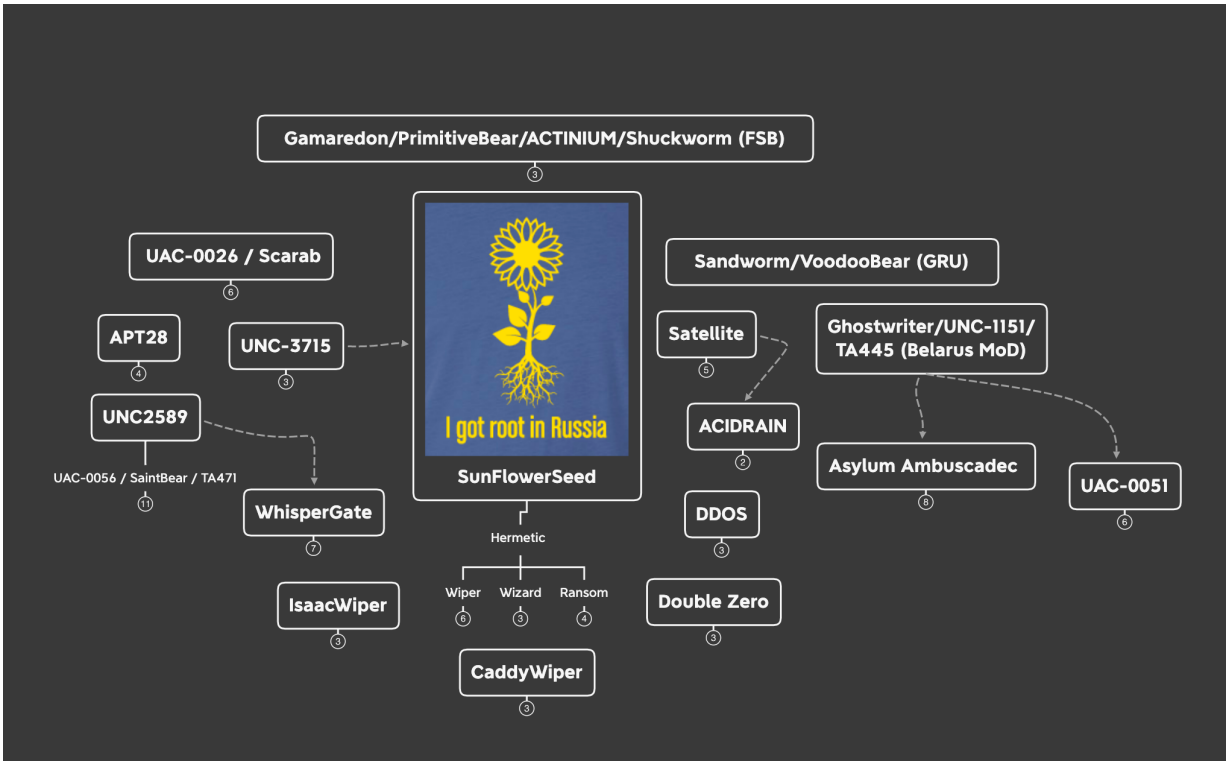
Tweeted March 4th, 2022

As the situation on the ground unfolded, so did developments on the cyber-front. The following tweet was shared to showcase the expanding landscape. Comparing the two graphics, we can see an uptick in threat actor activity targeting Ukraine. As seen in previous Russian movements and occupations of sovereign territory, physical movements tend to follow major pushes on the cyber-front, highlighting the value of threat actor support during military operations. Usually in the form of disrupting lines of communication and/or destabilizing regional infrastructure to "soften" the target for ground forces.



Tweeted March 18th, 2022

This last graphic is a condensed, "easy to swallow", form containing actors and threats observed up to the point of publication. (2022-04-12) Below we briefly touch on the major players and their roles in this conflict.



APT - SunFlowerSeed (NEARMISS/UNC-3715)

Threat activity produced by this actor leading to the physical invasion of Ukraine was the catalyst for focusing on Russian state sponsored/supporting threats and acted as a call to arms for the research community.

- Hermetic Wiper (FoxBlade/Trojan.KillDisk)
  Destructive malware with anti-forensic measures
- Hermetic Wizard - A worm that containing wiper characteristics
- Hermetic Ransom - Ransomware connected to PartyTicket and SonicVote

Ghostwriter/UNC-1151/TA445/UAC-0051 (Belarus MoD)

The current regime under Belarusian president Aleksandr Lukashenko has close relations to Vladimir Putin and his administration, allowing for Belarusian state assets to be (allegedly) deployed via their Ministry of Defense. The aim of this group is to operate disinformation campaigns regarding NATO credibility; targeting primarily Russian, Ukrainian and Polish speakers across different countries across Europe since 2017. Using spear-phishing tactics, Ghostwriter targeted members of Ukraine's armed forces to compromise their accounts and reach out to their contacts to cover and aid more destructive attacks conducted to further Russian state interests and the actions of associated APT groups.

MicroBackdoor

MicroBackdoor is an open source backdoor that is used for C2 communications. This means anyone may use this tool for various purposes and not just for attacks against Ukraine. Though extra features have been implemented by UAC-0051 not included in the open source version.

Asylum Ambuscade

This phishing campaign was observed operating within similar parameters as Ghostwriter/UNC-1151/TA445 activities, suggesting that this may be their work or the campaign may be connected through other means. At the time of publication, there were enough discrepancies to prevent conclusive attribution of this campaign to TA445. Primary targets chosen by Asylum Ambuscade operators differ from TA445 attributed attacks where TA445 pursued military personnel and organizations while Asylum Ambuscade set their sights on European government entities whose responsibilities are tied to transportation and logistics extending beyond military affairs such as refugee relief efforts.

APT28 (Fancy Bear)

This actor is attributed as the most prevalent and deeply connected of known Russian state sponsored actors. Their connection to GRU, the Russian military intelligence agency tasked with intelligence gathering and espionage beyond Russian territory alongside its civilian counterpart SVR, lends credibility to their activities and attacks being directly aligned with Russian state interests.

> Spear-phishing has been associated with APT28 activity using high volumes of compromised accounts along with newly created actor controlled infrastructure.

Activities directly related to the conflict in Syria, undermining Ukraine’s relations with NATO/member nations, and the 2016 U.S presidential election.

Sandworm/VoodooBear (GRU)

This group is also tied to GRU and handles matters related to targeting entities in the energy sector dating back to 2011. Along with espionage operations, Sandworm/VoodooBear is known for destructive malware deployed against industrial control and SCADA systems such as the 2015 attack against Ukraine’s energy sector leading to widespread blackouts.

- CyclopsBlink - Malicious Elf (Linux) executable.
  - Compiled for 32-bit PowerPC architecture
  - Large-scale botnet targeting Small Office/Home Office network devices (routers)
  - Encrypted C2 communication
  - Persistence via device firmware upgrade process

- Note: In early April 2022, the United States government secured a court order allowing for the removal of the malware from infected devices.

UNC-2589 (UAC-0056/SaintBear/TA471/Lorec53)

This threat group has been connected to spearphishing attempts targeting both Georgian and Ukrainian government entities using various malware. This group often targets government and critical infrastructure and tends to align with Russian state objectives, but is not confirmed with absolute certainty to be state sponsored.

- Saint_v3 - Trojan
- SaintBot - Malware Loader
- OutSteel - Document Stealer
- Elephant - Malware Framework
- GrimPlant - GO Backdoor
- GraphSteel - GO Backdoor
- Cobalt Strike Beacon - Default malware payload for Cobalt Strike

AcidRain (Likely connected to Sandworm)

This threat is attributed to the ELF modem wiper malware that was observed in connection to Viasat satellite attacks. Gaining access to Viasat's KA-SAT management infrastructure, attackers were able to push AcidRain to residential modems across Europe, effectively denying internet access to regions reliant on high-throughput satellite telecom service due to lack of traditional network infrastructure resources. As the various wipers seen prior to the physical invasion shed light on cyber offensive efforts and capabilities against Ukraine, AcidRain's impact reaches across Europe as far as disrupting remote communications to wind turbines in Germany. Along with surface level function similarities, AcidRain shares resemblance to VPNFilter malware at the code level, the predecessor to Cyclops Blink attributed to Sandworm. This suggests a deeper connection to Russian GRU assets rather than state sponsored activity.

[Update: 2022-04-18] Sandworm connection with medium confidence

UAC–0020/Vermin Group/SPECTR [Update: 2022-04-18]

A hacker collective associated with the Luhansk People's Republic (LPR), a breakaway faction/self proclaimed state officially designated as a terrorist organization by Ukraine. The Vermin group claims to represent "a security agency for the LPR" and has been linked to cybercrime activities aligned with Russian state goals prior to and leading into the invasion of Ukraine. This group is known for developing and deploying SPECTR malware, composed of several components/modules; targeting Ukrainian state entities.

UAC-0026/Scarab (China)

This group has been operational since 2012, possibly earlier, and is connected to Chinese threat actors that have used phishing emails with RAR attachments leading to HeaderTIP malware. Prior to the invasion, this group was observed targeting individuals worldwide; afterwards, setting their sites on targets within Ukraine using phishing lures bearing the National Police of Ukraine graphics and contact details claiming to be collecting video evidence of crimes committed by the Russian military.

- Deployed custom backdoor “Scieron”, believed to be an earlier iteration of HeaderTIP
- Observed to reuse C2 infrastructure from previous malware campaigns
- Known to craft lures specific to an individual target’s locale

UAC-0035/InvisiMole/LoadEdge/TunnelMole [Update: 2022-04-18]

This group has been observed conducting spear phishing attacks targeting Ukraine state organizations in accordance with Russian state aligned goals since 2013. Collaborative efforts with Gamaredon have also been seen via campaign overlap and one of the groups distributing payloads using distribution networks controlled by the other. InvisiMole is the name attributed to the spyware used to target their victims, which historically, have been Russian and Ukrainian military and diplomatic entities along with other organizations across eastern Europe. LoadEdge is a backdoor written in C++, also used by the group with various command and control capabilities. TunnelMole is the name attributed to their DNS tunnel malware used to externally retrieve additional data/payloads along with exfiltrating data covertly.

WhisperGate/DEV-0586

There are multiple WhisperGate campaigns as a result of overlap in attribution which is common within the research community. The most commonly referenced campaign is that of the destructive malware that corrupts an infected system’s master boot record and displays a fake ransomware note as the data is destroyed and cannot be recovered by paying the ransom. Microsoft Threat Intelligence Center (MSTIC) saw systems in Ukraine becoming infected on January 13, 2022; Likely done so in preparation for the ground invasion.

XakNet [Update: 2022-04-18]

This group is a hacker collective, composed of "Russian patriots" claiming to not hide behind the "mask of Anonymous" and vowing to retaliate against attacks targeting Russia by inflicting similar attacks against Ukrainian targets. Their most high profile act to date was leaking documents from Ukraine's Ministry of Foreign Affairs "exposing" a request for foreign aid in the form of equipment to protect from chemical exposure. Prior to the invasion of

Ukraine, this group openly advertised offering ethical hacking guidance and instruction; Afterwards stating that they are no longer teaching and defending, shifting to offensive efforts.

Gamaredon/PrimitiveBear/Armageddon/ACTINIUM/Shuckworm (FSB)

This actor has been actively targeting Ukrainian government entities since the “annex” of the Crimean peninsula by Russian forces in 2013. Observed in connection to Russian appointed FSB officers assigned to Crimea, the group gradually moved from deploying malware authored by other developers to their own custom payloads. Campaigns attributed to the actor show use of a combination of compromised Russian and Ukraine domains and IPs with autonomous systems for related IPs being physically located in Russia. A notable technique seen across their distribution network allows them to restrict access and requests with timed gates set to expire when domains rotate to a new IP; signaling the end of a particular run and impeding research efforts. Based on reports from the Security Service of Ukraine, the aim of this group is to obtain intelligence information from Ukrainian security, defense and law enforcement bodies via targeted campaigns.

CyberCrime:

In addition, we want to highlight crimeware activity, as many of these groups are associated with Russian threat actors. It is very interesting that some of the physical infrastructure utilized by cybercrime outfits are geographically located on U.S. soil and used against US citizens (along with other civilian targets worldwide) to not only access, but also collect funds that eventually end up back into the hands of Russian actors. Though previously the goal was simply to profit from ill-gotten gains, priorities have presumably shifted towards providing resources for Russian state assets.

Sanctions that were enacted onto Russia included a number of hosting providers as well as general internet access. This caused a heavy blow as it seemed to present issues with what some refer to as “commodity threats” that hit their inboxes daily such as IcedID, Dridex, Hancitor, Qbot, Trickbot, etc. This was initially easing the burden for community individuals to focus on other threats and make connections to less popular named threats along with analysts that have to track all of this activity. The break was short lived and now we are seeing these actors resume operations after some retooling on their infrastructure and/or access to their boxes.

Parting Words:

Though this is not an exhaustive list, the content provided reveals enough to highlight where our collective gaps lie and where efforts should be focused to undermine the efforts tied to the Russian state. As previously mentioned, further developments will be added to this article as the situation continues to unfold. Our list of sources below may include actors and threats

to be summarized later as we gather more information and form more concrete attributions. Feel free to reach out to us with suggestions for content and information to include or elaborate on. At the time of publication, Ukrainian morale stood high as Russian military forces seemed to present itself as a paper tiger, especially in the face of the smaller Ukrainian force backed by military aid from allied nations across the globe. It is critical that global efforts on the cyber-front maintain the same unified stance if we hope to see this conflict come to a swift end and prevent any potential escalations.

Sources

UNC-3715
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation

AcidRain
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

WhisperGate/DEV-0586
https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

Tags

Get The InQuest Insider

Find us on Twitter for frequent updates, follow our Blog for bi-weekly technical write-ups, or subscribe here to receive our monthly newsletter, The InQuest Insider. We curate and provide you with the latest news stories, field notes about innovative malware, novel research / analysis / threat hunting tools, security tips and more.