US arrests Latvian woman who worked on Trickbot malware source code

therecord.media/us-arrests-latvian-woman-who-worked-on-trickbot-malware-source-code/

June 4, 2021

The US Department of Justice has arraigned in court today a Latvian woman who was part of the Trickbot malware crew, where she served as a programmer and wrote code for controlling the malware and deploying ransomware on infected computers.

Alla Witte, 55, of Latvia, but who resided in Paramaribo, Suriname, was arrested on February 6 in Miami, Florida, the DOJ said in a press release today.

US officials said that Witte, who went online as “Max,” has been working with the Trickbot malware gang since the group formed in November 2015, when remnants of the Dyre malware gang assembled to create and distribute a revamped version of the Dyre trojan that was subsequently named Trickbot.

According to court documents [PDF], Witte was identified as one of 17 suspects behind the Trickbot malware, which is belived to have infected millions of computers across the world since 2015.

US investigators said Witte oversaw “the creation of code related to the monitoring and tracking of authorized users of the Trickbot malware, the control and deployment of ransomware, obtaining payments from ransomware victims, and developing tools and

protocols for the storage of credentials stolen and exfiltrated from victims infected by Trickbot."

Her role in the Trickbot gang evolved as the malware also changed—which went from a classic **banking trojan** focused on stealing funds from bank accounts to a **loader** for other malware payloads (such as ransomware operations).

US officials have charged Witte in 19 counts in a 47-count indictment. Public comments from cybersecurity professionals suggest that Witte did not did a good job at hiding her identity, even hosting in-dev versions of the Trickbot malware on her personal website.

> 👋👋Tango down: "Alla Witte" aka "Alla Klimova" – one known #TrickBot developer and operator arrested!
>
> 📌She previously hosted even TrickBot "red" group tag payload on her own website -> see URLhaus https://t.co/8LwtzBSZGRhttps://t.co/Nby4k2jvnt pic.twitter.com/qG977wjgLN
>
> — Vitali Kremez (@VK_Intel) June 4, 2021

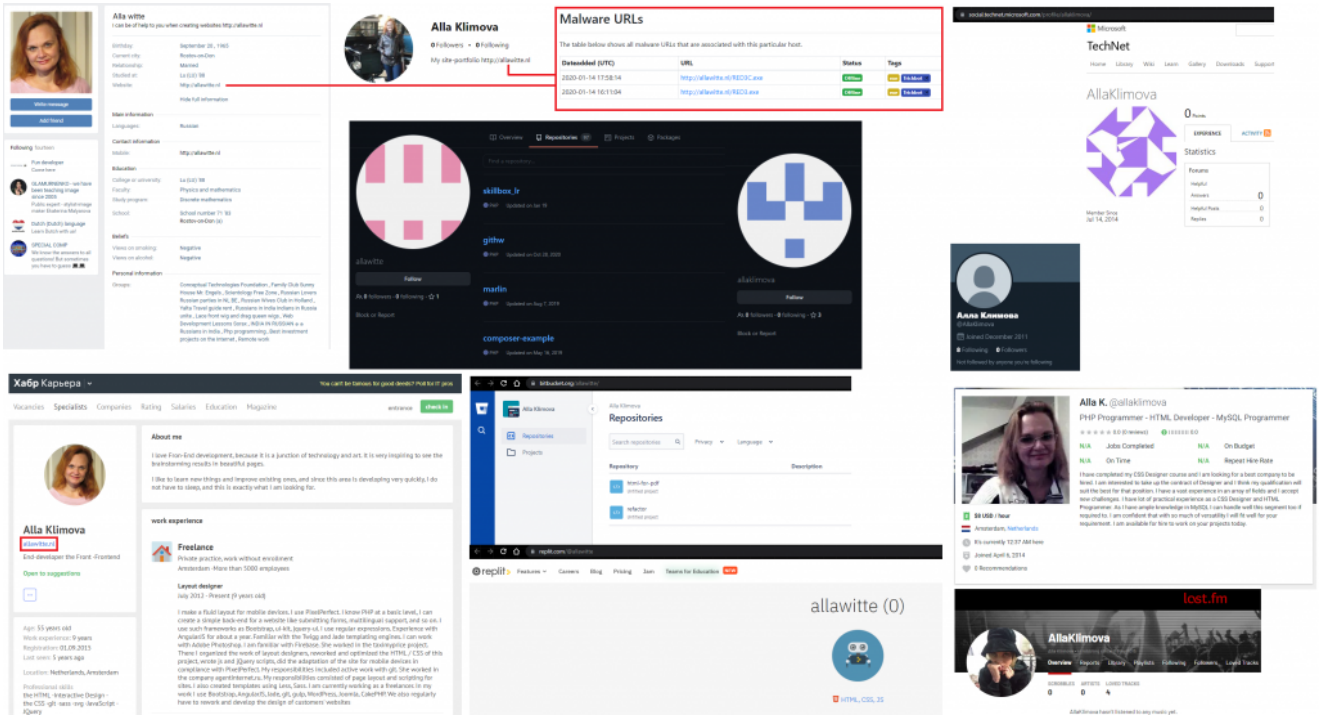

Image: William Thomas, Cyjax

Witte is the first member of the Trickbot gang to be arrested. US officials said other Trickbot suspects are still at large in Russia, Belarus, Ukraine, and Suriname.

In October 2020, US officials filed charges against a criminal group known as QQAAZZ that helped the Trickbot gang launder funds they stole from victims' bank accounts.

In the same month, a coalition of tech companies attempted to take down the Trickbot botnet. While the Trickbot gang's operation were disrupted for a few weeks, the botnet has since recovered and is still active today.

What is Trickbot

Historically, the Trickbot botnet is one of the largest and most successful operations to date.

It began operations in 2015 after members of the Dyre malware gang scattered following a series of high-profile arrests that crippled the group's leadership structure.

Trickbot was set up as an alternative and initially it continued where Dyre left off, with its operators investing most of their time in email spam campaigns aimed at tricking users into downloading and installing the malware on their computers.

In its early history, Trickbot worked as a classic banking trojan that infected computers and then tampered with users browsers' to dump and steal credentials, and then show "web injects" that allowed the gang to collect e-banking credentials and interact with e-bank accounts in real-time.

However, as banks began deploying security features that made the life of banking trojans harder, circa 2017, the Trickbot gang followed other malware groups that were active at the time and converted their banking trojan into a simpler and leaner malware strain. Known as a loader (from down**loader**) or dropper, Trickbot would continue to infect victims with the help of email spam, but once it infected a host, it's primary purpose would be to download and install other malware strains.

This way, throughout the years, the Trickbot gang built a giant botnet to which they sold access to other criminal groups. Known as a Crimeware-as-a-Service, Trickbot operators allowed customers to deploy their own malware or created specialized modules that customers could deploy for specific tasks.

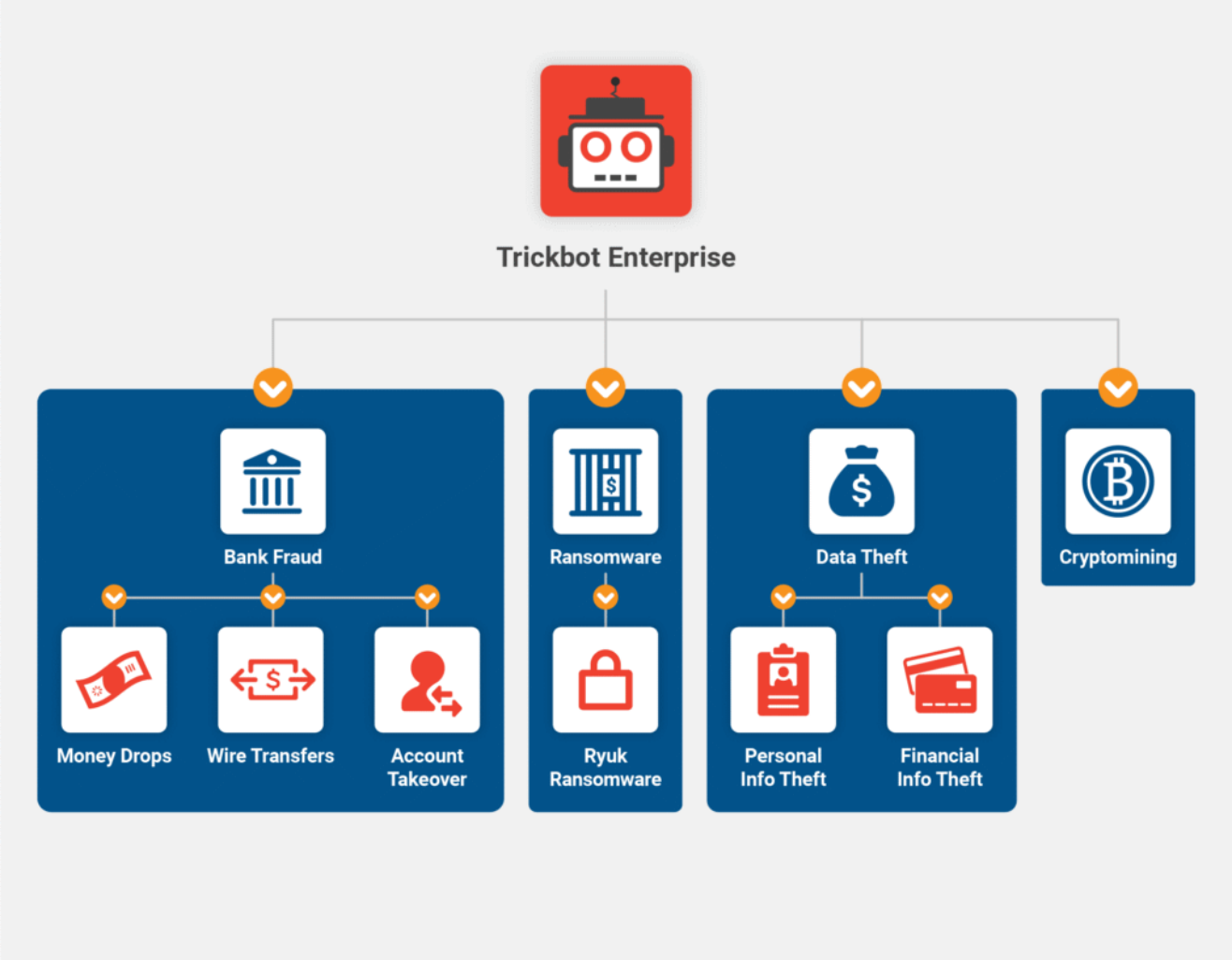

Image: Eclypsium

Depending on the victims they infected, the Trickbot malware was often used to steal banking credentials, passwords for enterprise networks, give BEC scammers an entry into large companies, allow data brokers to pilfer secrets and sensitive files from corporate networks, or even deploy ransomware , such as Ryuk and Conti, for destructive attacks.

After it survived its takedown last year and after the Emotet takedown earlier this year, Trickbot is now considered one of the most dangerous botnets active today, together with Dridex, Qbot, and IcedID.

The court documents filed in Witte's case today are heavily redacted to hide the name of the other 16 Trickbot operators, suggesting US officials are aware of their identities already and that future arrests and charges are bound to follow.

Tags

- banking trojan
- cybercrime
- developer
- malware

- Ransomware
- source code
- Trickbot

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.