'Anomalous' spyware stealing credentials in industrial firms

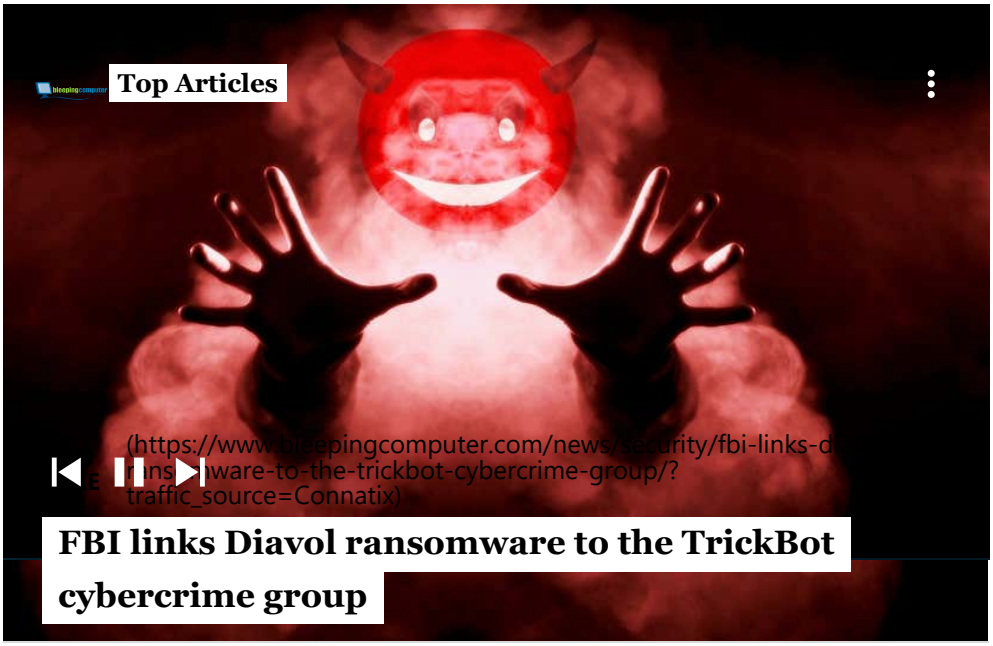
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

January 20, 2022 04:29 PM **0**

Researchers have uncovered several spyware campaigns that target industrial enterprises, aiming to steal email account credentials and conduct financial fraud or resell them to other actors.

The actors use off-the-shelf spyware tools but only deploy each variant for a very limited time to evade detection.

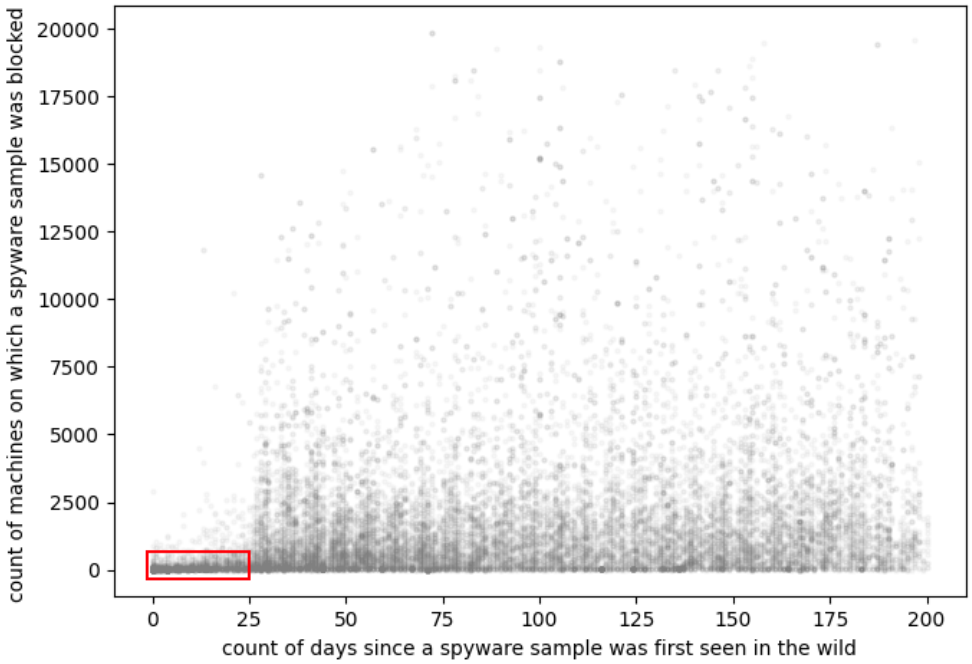
Examples of commodity malware used in attacks include AgentTesla/Origin Logger, HawkEye, Noon/Formbook, Masslogger, Snake Keylogger, Azorult, and Lokibot.



An atypical attack

Kaspersky calls these spyware attacks 'anomalous' because of their very short-lived nature compared to what is considered typical in the field.

More specifically, the lifespan of the attacks is limited to roughly 25 days, whereas most spyware campaigns last for several months or even years.



Duration of the attacks compared to stats from all detections

Source: Kaspersky

The number of attacked systems in these campaigns is always below one hundred, half of which are ICS (integrated computer systems) machines deployed in industrial environments.

Another unusual element is using the SMTP-based communication protocol for exfiltrating data to the actor-controlled C2 server.

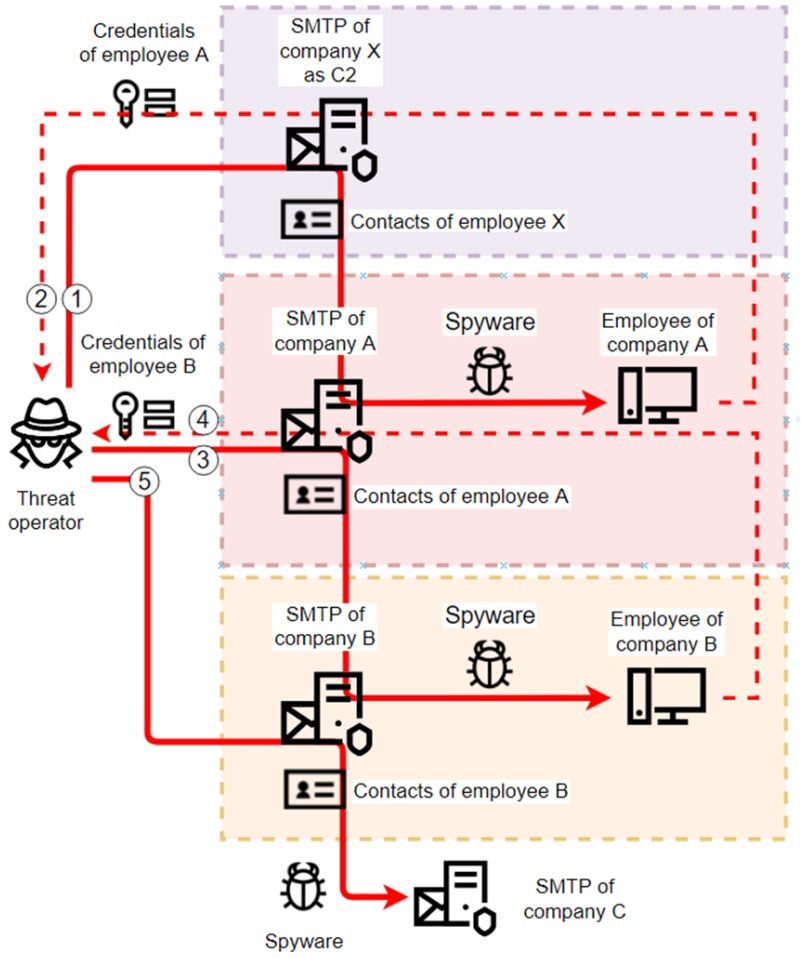
Unlike HTTPS, which is used in most standard spyware campaigns for C2 communication, SMTP is a one-way channel that caters only to data theft.

SMTP isn't a common choice for threat actors because it can't fetch binaries or other non-text files, but it thrives through its simplicity and ability to blend with regular network traffic.

Stealing credentials to further the infiltration

The actors use stolen employee credentials that they acquire via spear-phishing to infiltrate deeper and move laterally in the company's network.

Moreover, they use corporate mailboxes compromised in previous attacks as C2 servers to new attacks, making the detection and flagging of malicious internal correspondence very challenging.



Operational diagram
Source: Kaspersky

"Curiously, corporate antispam technologies help the attackers stay unnoticed while exfiltrating stolen credentials from infected machines by making them 'invisible' among all the garbage emails in spam folders." - explains Kaspersky's report (https://securelist.com/hunt-for-corporate-credentials-on-ics-networks/105545/)

In terms of numbers, the analysts identified at least 2,000 corporate email accounts abused as temporary C2 servers and another 7,000 email accounts abused in other ways.

Selling on dark web markets

Many of the email RDP, SMTP, SSH, cPanel, and VPN account credentials stolen in these campaigns are posted on dark web marketplaces and eventually sold to other threat actors.

According to Kaspersky's statistic analysis, around 3.9% of all RDP accounts sold in these illegal markets belong to industrial companies.

RDP (remote desktop protocol) accounts are precious to cybercriminals because they enable them to remotely access the compromised machines and directly interact with a device without raising any red flags.

Typically, these listings trigger the interest of ransomware actors who use RDP access to deploy their devastating malware.