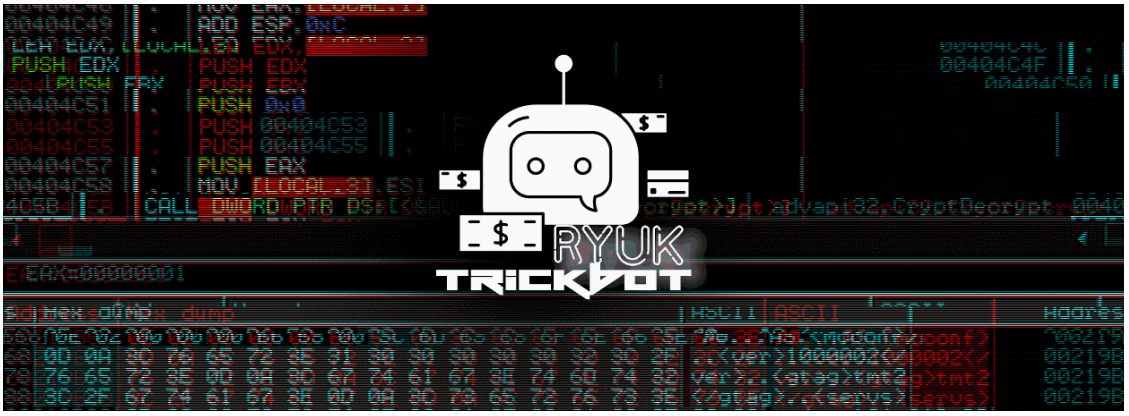
Ryuk ransomware deployed two weeks after Trickbot infection

By Ionut Ilascu

Published: 2020-06-23 · Archived: 2026-04-05 16:15:58 UTC

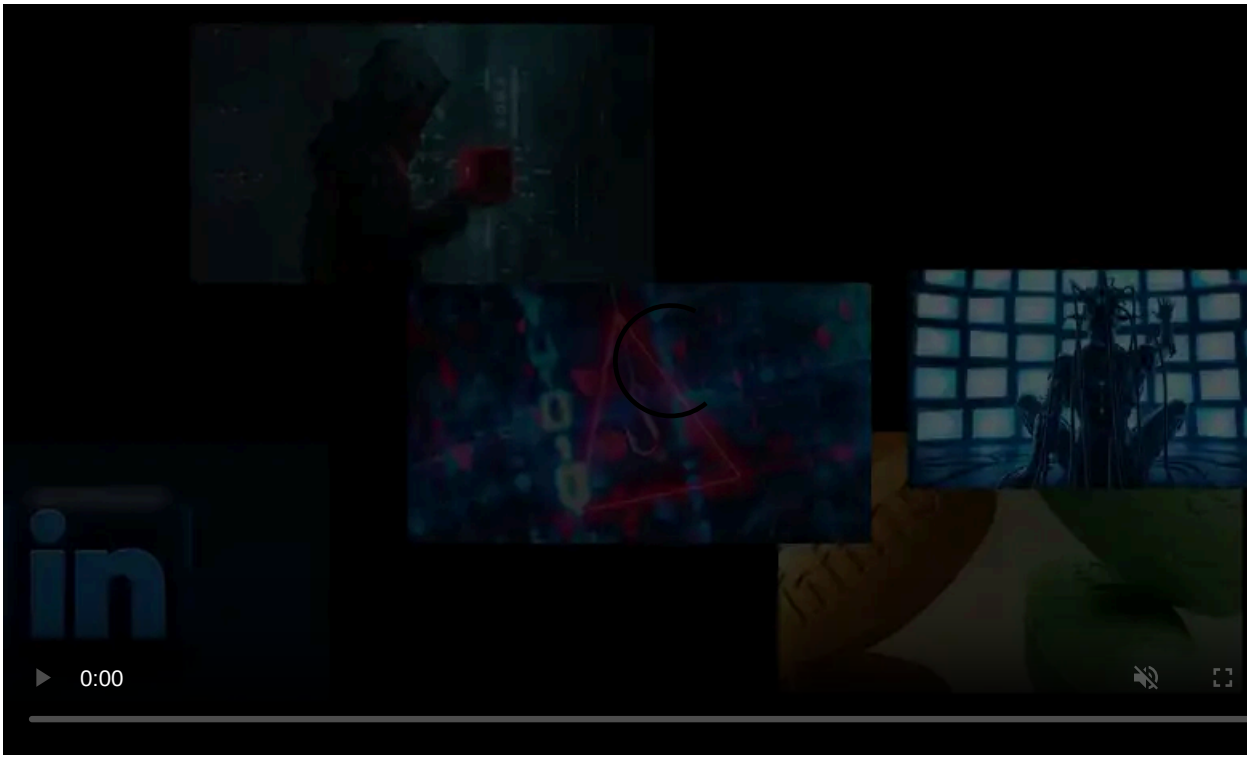


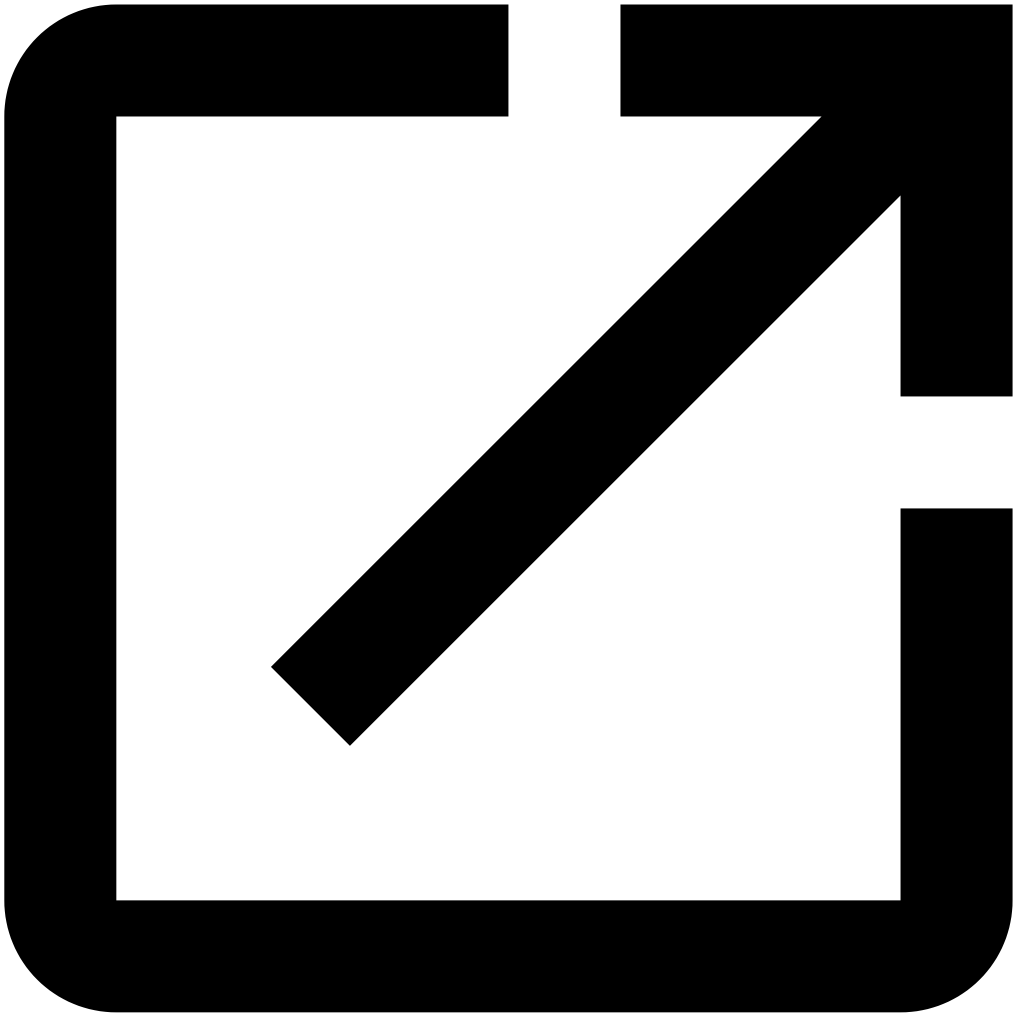
Activity logs on a server used by the TrickBot trojan in post-compromise stages of an attack show that the actor takes an average of two weeks pivoting to valuable hosts on the network before deploying Ryuk ransomware.

After compromising the network, the attacker starts scanning for live systems that have specific ports open and stealing password hashes from the Domain Admin group.

Manual hacking

Researchers at SentinelOne have detailed the activity observed from logs on a Cobalt Strike server that TrickBot used to profile networks and systems.


0:00



Once the actor took interest in a compromised network, they used modules from Cobalt Strike threat emulation software for red teams and penetration testers.

One component is the DACheck script to check if the current user has Domain Admin privileges and check the members of this group. They also used Mimikatz to extract passwords that would help with lateral movement.

```
10/07 23:18:11 UTC [task] <T1086, T1064> Tasked beacon to import: /root/CobaltStrike-ToolKit/Invoke-DACheck.ps1
10/07 23:18:11 UTC [task] <T1086> Tasked beacon to run: Invoke-DACheck -Initial True
10/07 23:18:11 UTC [task] <T1134, T1050> Tasked beacon to get SYSTEM
10/07 23:18:11 UTC [indicator] service: \\127.0.0.1 upd42d44
10/07 23:18:11 UTC [task] <T1003, T1055, T1093> Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
```

The researchers found that discovering computers of interest on the network is done by scanning for live hosts that have specific ports open.

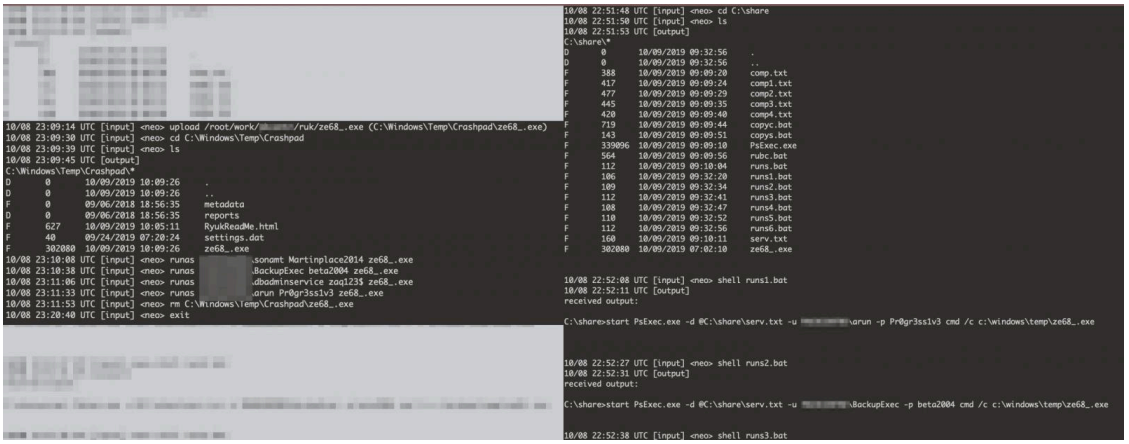
Services like FTP, SSH, SMB, SQL server, remote desktop, and VNC are targeted because they help move to other computers on the network or indicate a valuable target.

```
10/07 23:20:32 UTC [input] <neo> portscan 192.168.168.0-192.168.168.255 21,22,445,1433,3389,5900 icmp 1024
10/07 23:20:33 UTC [task] <T1046, T1093>
Tasked beacon to scan ports 21,22,445,1433,3389,5900 on 192.168.168.0-192.168.168.255
```

Dropping Ryuk

According to SentinelOne's examination, the threat actor profiles each machine to extract as much useful information as possible. This allows them to take complete control of the network and get access to as many hosts as possible.

Reconnaissance and pivoting stages are followed by planting Ryuk ransomware and deploying it to all accessible machines using Microsoft's PsExec tool for executing processes remotely.



Based on the timestamps, SentinelOne researchers estimate that it took two weeks for the attacker to gain access to machines on the network and profile them before executing Ryuk.

Vitali Kremez of Advanced Intelligence (AdvIntel) security boutique told BleepingComputer that this average for the "incubation" period is accurate, although it varies from one victim to another.

In some cases, Ryuk was deployed after just one day, while in other instances the file-encrypted malware was executed after the attacker had spent months on the network.

Kremez told us that Ryuk infections have slowed down lately, as the threat actor is likely in a vacation kind of state.

It is important to note that not all TrickBot infections are followed by Ryuk ransomware, probably because the actors take the time to analyze the data collected and determine if the victim is worth encrypting or not.
