Linux warning: TrickBot malware is now infecting your systems

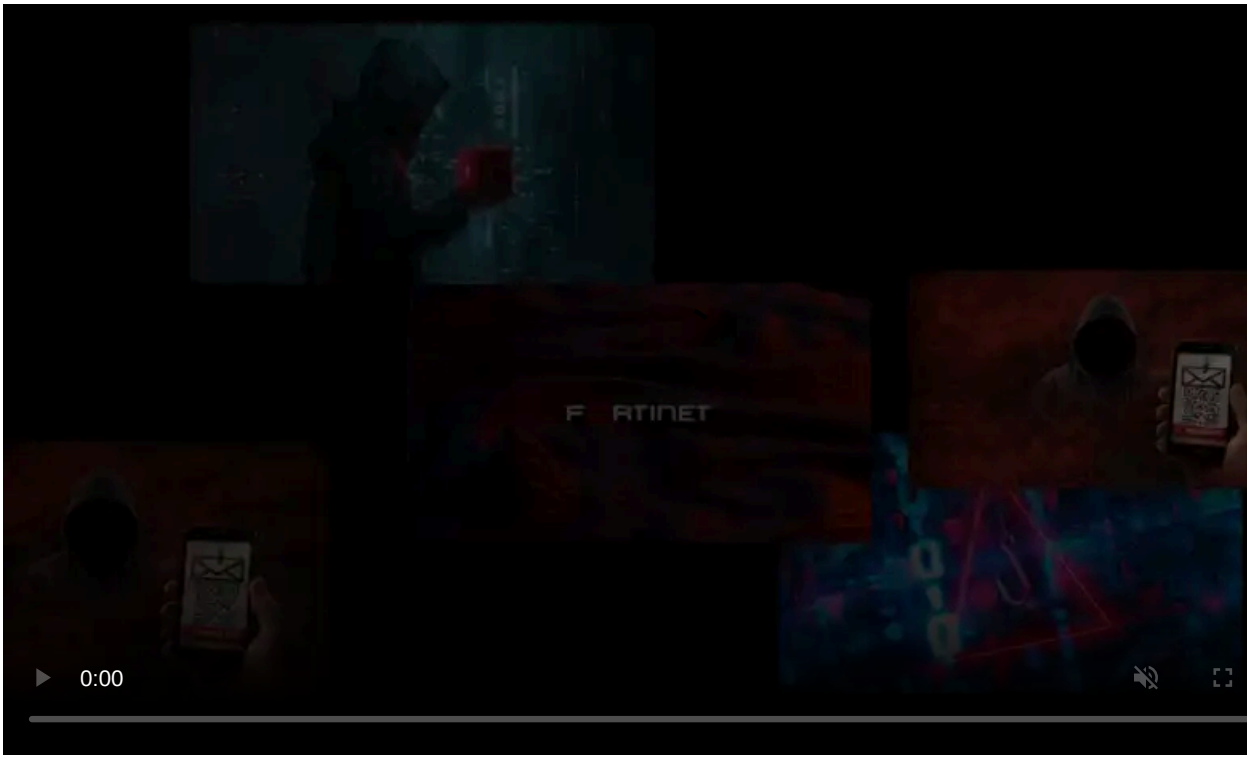
By Lawrence Abrams

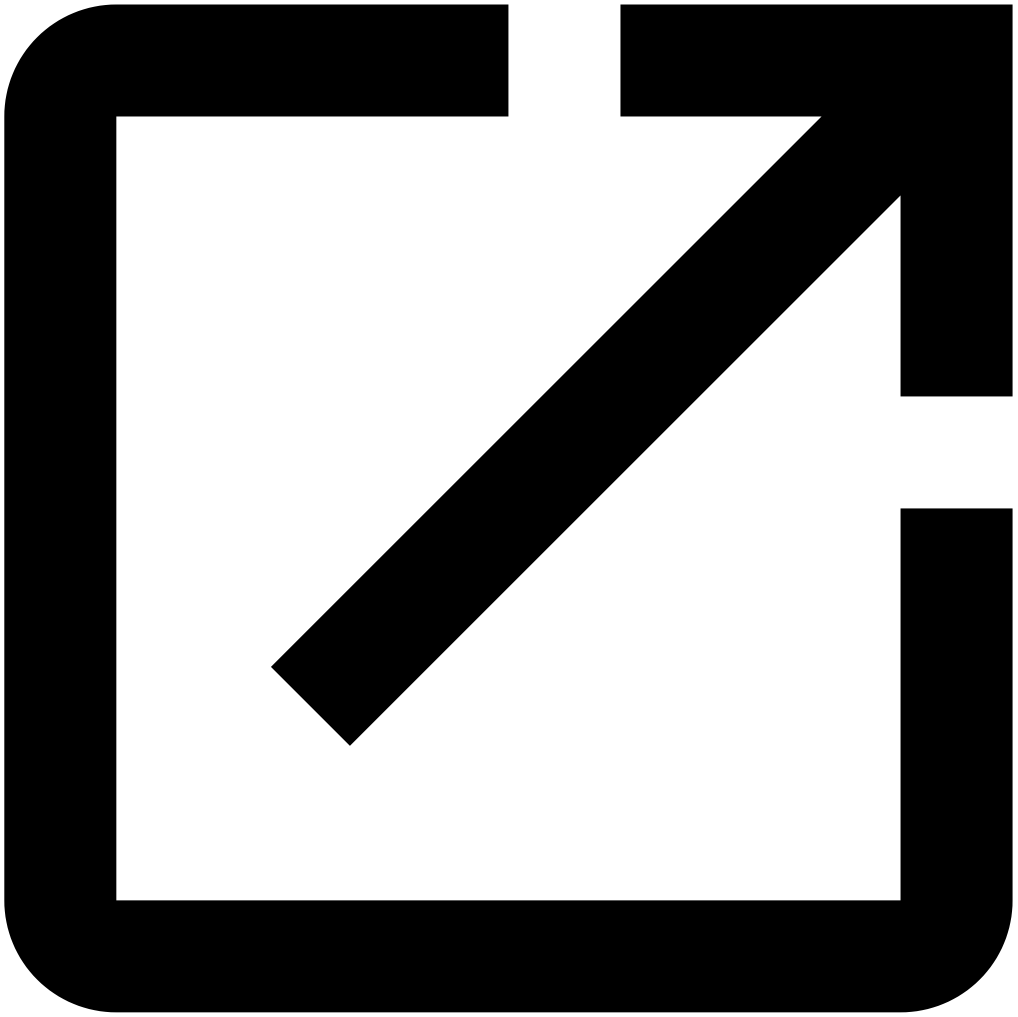
Published: 2020-07-31 · Archived: 2026-04-05 22:43:04 UTC

7/31/20: Update added below with information from Intezer Labs and a link to the malware sample. This article was originally published on July 30th, 2020.

TrickBot's Anchor malware platform has been ported to infect Linux devices and compromise further high-impact and high-value targets using covert channels.

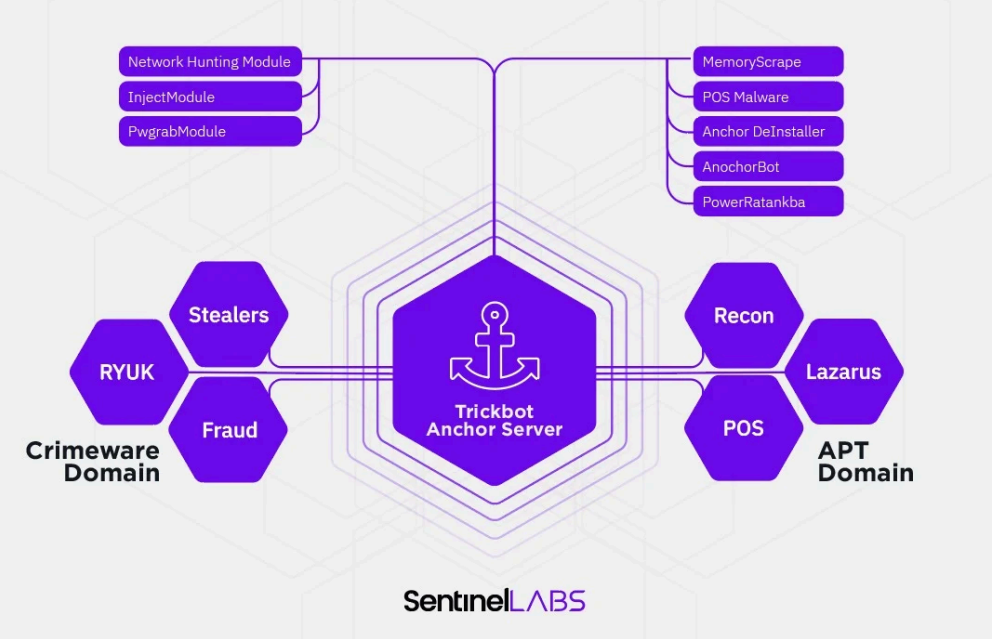
TrickBot is a multi-purpose Windows malware platform that uses different modules to perform various malicious activities, including information stealing, password stealing, Windows domain infiltration, and malware delivery.


F RTINET
0:00



TrickBot is rented by threat actors who use it to infiltrate a network and harvest anything of value. It is then used to deploy ransomware such as Ryuk and Conti to encrypt the network's devices as a final attack.

At the end of 2019, both SentinelOne and NTT reported a new TrickBot framework called Anchor that utilizes DNS to communicate with its command and control servers.



TrickBot's Anchor framework
Source: SentinelOne

Named Anchor_DNS, the malware is used on high-value, high-impact targets with valuable financial information.

In addition to the ransomware deployments via Anchor infections, the TrickBot Anchor actors also use it as a backdoor in APT-like campaigns that target point-of-sale and financial systems.

TrickBot's Anchor backdoor malware is ported to Linux

Historically, Anchor has been a Windows malware. Recently a new sample has been discovered by Stage 2 Security researcher Waylon Grange that shows that Anchor_DNS has been ported to a new Linux backdoor version called 'Anchor_Linux.'

Anchor_Linux string found in x64 Linux executable
Source: Waylon Grange

Advanced Intel's Vitali Kremez analyzed a sample of the new Anchor_Linux malware found by Intezer Labs.

Kremez told BleepingComputer that, when installed, Anchor_Linux will configure itself to run every minute using the following crontab entry:

```
*/1 * * * * root [filename]
```

```
15
16  v1 = needle;
17  *(_QWORD *)dest = 0LL;
18  qmemcpy(&filename, "/etc/crontab", 0xDuLL);
19  v2 = &v13;
20  for ( i = 1020LL; i; --i )
21  {
22    *(_DWORD *)v2 = 0;
23    v2 += 4;
24  }
25  strcat(dest, "*/1 *\t* * *\troot\t");
26  strcat(dest, v1);
27  v4 = fopen(&filename, "a+");
28  if ( v4 )
29  {
```

Setting up persistence via CRON

Source: Vitali Kremez

In addition to acting as a backdoor that can drop malware on the Linux device and execute it, the malware also contains an embedded Windows TrickBot executable.

property	value
size	936
format	Unknown
stamp	Thu Dec 19 11:06:59 2019
path	n/a

Embedded Windows executable

Source: Vitali Kremez

According to Intezer, this embedded binary is a new light-weight TrickBot malware "with code connections to older TrickBot tools" and is used to infect Windows machines on the same network.

To infect Windows devices, Anchor_Linux will copying the embedded TrickBot malware to Windows hosts on the same network using SMB and $IPC.

When successfully copied to a Windows device, Anchor_Linux will configure it as a Windows service using the Service Control Manager Remote protocol and the SMB SVCCTL named pipe.

```
cVar1 = smb2_connect(smb_ctx,param_2,"IPC$");
if ((cVar1 != '\0') && (lVar3 = smb2_open(*smb_ctx,"svcctl",2), lVar3 != 0)) {
  iVar2 = smb2_write(*smb_ctx,lVar3,&smb_cmd_struct,0x48);
  if ((iVar2 == 0x48) && (iVar2 = smb2_read(*smb_ctx,lVar3,local_1038,0x1000), -1 < iVar2)) {
    __ptr = (void **)alloc(0xc);
                    /* try { // try from 00415999 to 0041599d has its CatchHandler @ 00415d90 */
    FUN_00414f5c(__ptr,2,param_2);
    iVar2 = smb2_write(*smb_ctx,lVar3,*__ptr,(ulong)*(uint *)(__ptr + 1));
    if (iVar2 < 0) {
      uVar4 = 0;
    }
```

Copying a file via SMB

Source: Waylon Grange

When the service is configured, the malware is started on the Windows host, connecting back to the command and control server for commands to execute.

This Linux version allows threat actors to target non-Windows environments with a backdoor that lets the attackers covertly pivot to Windows devices on the same network.

"The malware acts as covert backdoor persistence tool in UNIX environment used as a pivot for Windows exploitation as well as used as an unorthodox initial attack vector outside of email phishing. It allows the group to target and infect servers

in UNIX environment (such as routers) and use it to pivot to corporate networks," Kremez told BleepingComputer in a conversation about the malware.

Even worse, many IoT devices such as routers, VPN devices, and NAS devices run on Linux operating systems, which could potentially be a target for Anchor_Linux.

With this evolution of the TrickBot malware, it is increasingly important for Linux systems and IoT devices to have adequate protection and monitoring to detect threats like Anchor_Linux

For Linux users concerned, they may be infected, Anchor_Linux will create a log file at `/tmp/anchor.log`. If this file exists, you should perform a complete audit of the system for the presence of the Anchor_Linux malware.

Kremez told BleepingComputer that he believes that Anchor_Linux is still in development due to testing functionality in the Linux executable.

It is expected that TrickBot will continue its development to make it a full-featured addition to its Anchor framework.

Source: https://www.bleepingcomputer.com/news/security/trickbots-new-linux-malware-covertly-infects-windows-devices/