Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices

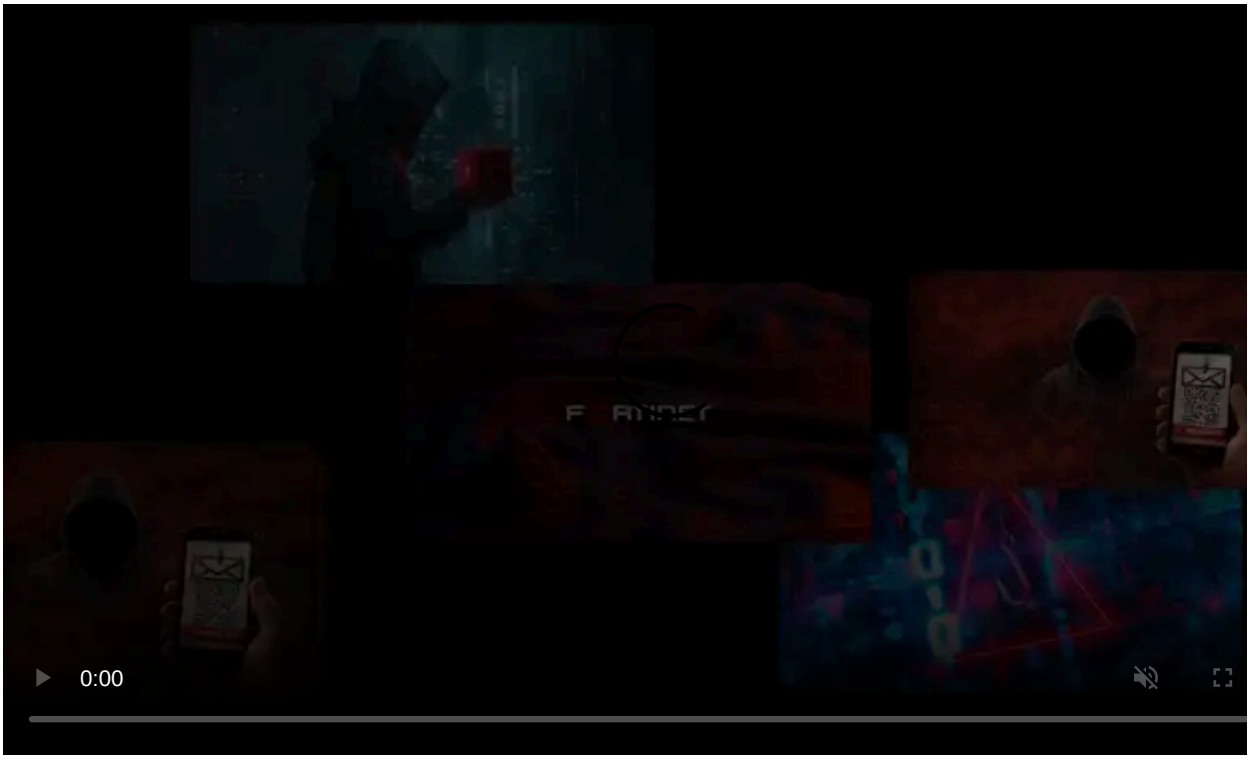
By Lawrence Abrams

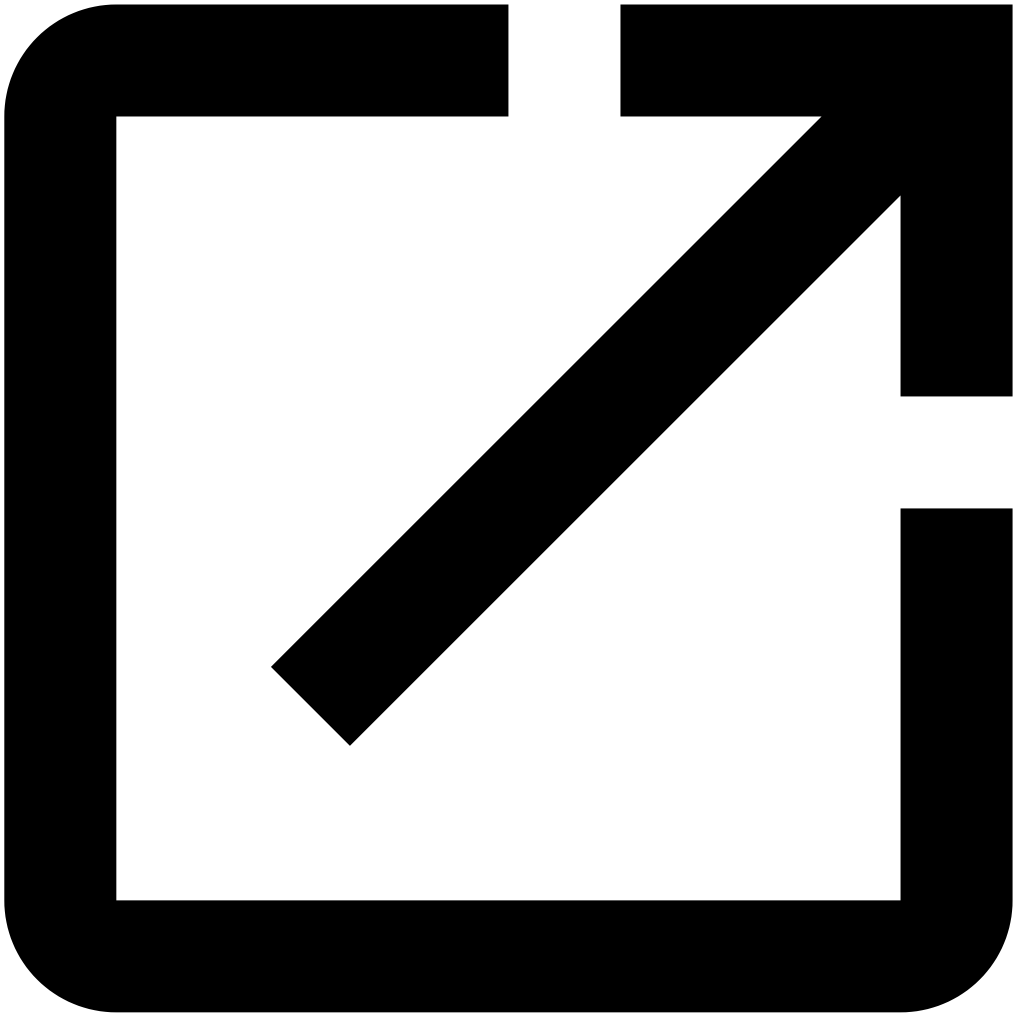
Published: 2020-01-14 · Archived: 2026-04-05 21:09:46 UTC

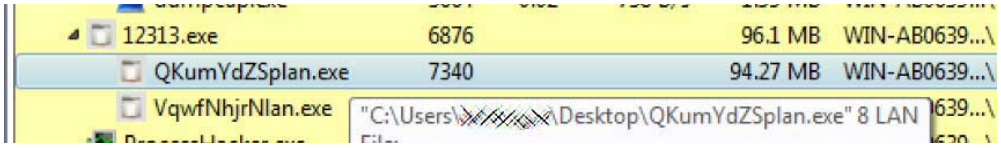
The Ryuk Ransomware uses the Wake-on-Lan feature to turn on powered off devices on a compromised network to have greater success encrypting them.

Wake-on-Lan is a hardware feature that allows a powered down device to be woken up, or powered on, by sending a special network packet to it. This is useful for administrators who may need to push out updates to a computer or perform scheduled tasks when it is powered down.

According to a recent analysis of the Ryuk Ransomware by Head of SentinelLabs Vitali Kremez, when the malware is executed it will spawn subprocesses with the argument '8 LAN'.


0:00





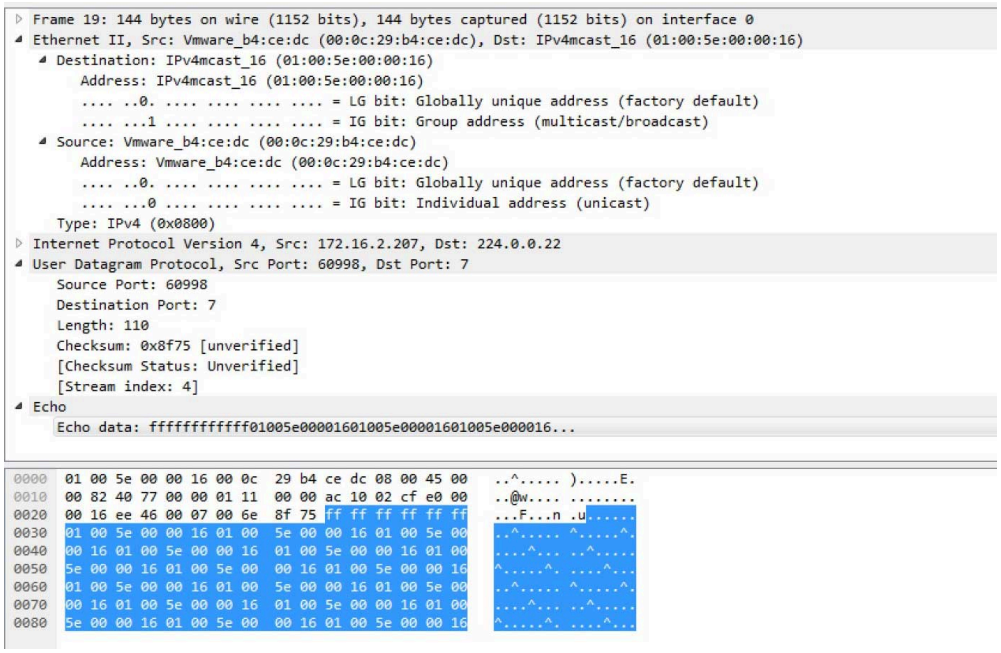
Spawning subprocess with 8 Lan argument

When this argument is used, Ryuk will scan the device's ARP table, which is a list of known IP addresses on the network and their associated mac addresses, and check if the entries are part of the private IP address subnets of "10.", "172.16.", and "192.168."

```
53      if ( v6 )
54      {
55        while ( 1 )
56        {
57          sub_3500A453((_WORD **)(v6 + 12), (int)&cp);
58          if ( (char *)arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)&byte_350111A8) == &cp// 10.
59            || arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)"172.16.")
60            || arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)"192.168.") )
61          {
62            v35 = inet_addr(&cp);
63            if ( v35 == 0xFFFFFFFF )
64              return 0xFFFFFFFF;
65            sub_350018CA(*(_BYTE *)(v6 + 44), &v24);
66            v34 = (unsigned __int64)(((255 - BYTE1(v24)) << 16)
67                                   + (signed int)((0xFFFFFFFF - (unsigned __int8)v24) << 24)
68                                   + (signed __int64)((255 - BYTE2(v24)) << 8)) >> 32;
69            v7 = ((255 - BYTE1(v24)) << 16) + ((0xFFFFFFFF - (unsigned __int8)v24) << 24) + ((255 - BYTE2(v24)) << 8);
70            v23 = 255 - BYTE3(v24) + v7;
71            v8 = 255 - BYTE3(v24) + __PAIR__(v34, v7);
72            v9 = __CFADD__((_DWORD)v8, *(_DWORD *)v3);
73            *(_DWORD *)v3 += v8;
74            v34 = HIDWORD(v8);
75            *(_DWORD *)(v3 + 4) += HIDWORD(v8) + v9;
76            if ( v8 >= 0xFF )
77              v10 = 0;
78            else
79              v10 = BYTE3(v35);
```

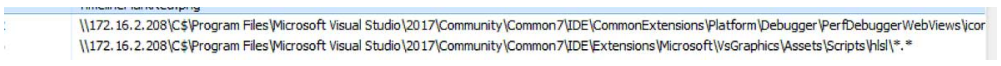
Checking for private network

If the ARP entry is part of any of those networks, Ryuk will send a Wake-on-Lan (WoL) packet to the device's MAC address to have it power up. This WoL request comes in the form of a 'magic packet' containing 'FF FF FF FF FF FF FF FF'.



Ryuk sending a WoL packet

If the WoL request was successful, Ryuk will then attempt to mount the remote device's C$ administrative share.



Mount drive to the Remote C$ Share

If they can mount the share, Ryuk will encrypt that remote computer's drive as well.

In conversations with BleepingComputer, Kremez stated that this evolution in Ryuk's tactics allow a better reach in a compromised network from a single device and shows the Ryuk operator's skill traversing a corporate network.

"This is how the group adapted the network-wide ransomware model to affect more machines via the single infection and by reaching the machines via WOL & ARP," Kremez told BleepingComputer. "It allows for more reach and less isolation and demonstrates their experience dealing with large corporate environments."

To mitigate this new feature, administrators should only allow Wake-on-Lan packets from administrative devices and workstations.

This would allow administrators to still benefit from this feature while adding some security to the endpoints.

At the same time, this does not help if an administrative workstation is compromised, which happens quite often in targeted ransomware attacks.

Update 1/14/20 11:28 AM: CrowdStrike also has analysis of this feature here.

Source: https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/