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

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

Lawrence Abrams

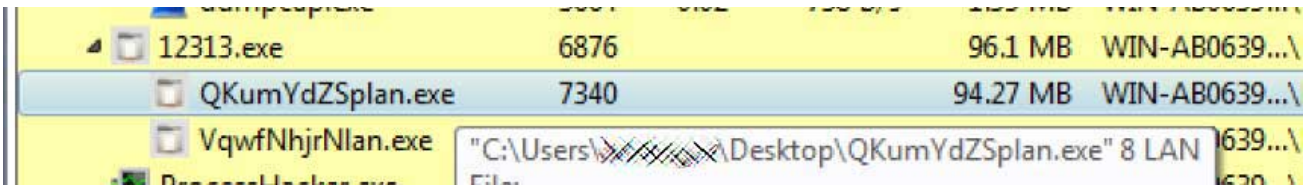
By
Lawrence Abrams

- January 14, 2020
- 03:30 AM
- 5

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'.



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_35004453((_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

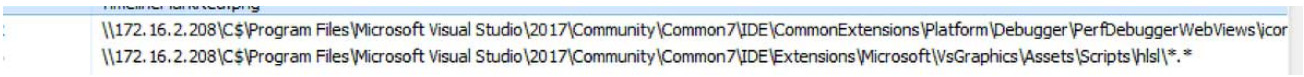
If the ARP entry is part of any of those networks, Ryuk will send a Wake-on-Lan (WoL) packet to the device's MAC address to have it power up. This WoL request comes in the form of a 'magic packet' containing 'FF FF FF FF FF FF FF FF'.

```
▷ Frame 19: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
◢ Ethernet II, Src: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
  ◢ Destination: IPv4mcast_16 (01:00:5e:00:00:16)
      Address: IPv4mcast_16 (01:00:5e:00:00:16)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ◢ Source: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
      Address: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 172.16.2.207, Dst: 224.0.0.22
◢ User Datagram Protocol, Src Port: 60998, Dst Port: 7
    Source Port: 60998
    Destination Port: 7
    Length: 110
    Checksum: 0x8f75 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
◢ Echo
    Echo data: ffffffffffff01005e00001601005e00001601005e000016...
```

```
0000  01 00 5e 00 00 16 00 0c  29 b4 ce dc 08 00 45 00   ..^..... ).....E.
0010  00 82 40 77 00 00 01 11  00 00 ac 10 02 cf e0 00   ..@w.... ........
0020  00 16 ee 46 00 07 00 6e  8f 75 ff ff ff ff ff ff   ...F...n .u......
0030  01 00 5e 00 00 16 01 00  5e 00 00 16 01 00 5e 00   ..^..... ^.....^.
0040  00 16 01 00 5e 00 00 16  01 00 5e 00 00 16 01 00   ....^... ..^.....
0050  5e 00 00 16 01 00 5e 00  00 16 01 00 5e 00 00 16   ^.....^. ....^...
0060  01 00 5e 00 00 16 01 00  5e 00 00 16 01 00 5e 00   ..^..... ^.....^.
0070  00 16 01 00 5e 00 00 16  01 00 5e 00 00 16 01 00   ....^... ..^.....
0080  5e 00 00 16 01 00 5e 00  00 16 01 00 5e 00 00 16   ^.....^. ....^...
```

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.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- ARP
- Packet
- Ransomware
- Ryuk
- Wake-on-LAN
- WoL

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  navidas73 - 2 years ago
  -
  -
  Terrifying how much criminal energy goes into the development of RYUK ransomware.

- 
  Alovalovayea - 2 years ago
  -
  -
  Hello, i've found SEVERAL WAYS to recover Ryuk encrypted files. I would be glad if anyone could give me some sample because it could be useful in finding a way to calculate the key instead of just recovering files. This ransomware is so advanced (in terms of his code and process) that they forgot about some SIMPLE WINDOWS'S ENVIROMENTS things that are helpful in recovering files.

- 
  buddy215 - 2 years ago
  -
  -
  Other than using external backup copies of files encrypted on the computer....what other way have you found for "recovering" encrypted files other than decryting? Inquiring minds want to know.

- 
  Alovalovayea - 2 years ago
  -
  -
  Just to tell you something, working on file history could let you recover everything on a company network. Every workstation can help you decrypt another workstation, but I can't give you details for now. Talking about any other method, would result on helping the hacker team behind ryuk and that's why I want to use my samples (and some more, If can get some) to calculate the key (it's not that difficult understanding how if you analyze the infection through a network sniffer on a sandbox)

- 
  Alovalovayea - 2 years ago
  -
  -
  Sodinokibi (post August 2019 version) successfully decrypted thanks to a Facebook group who submitted samples. Ryuk's taking a bit more time but it's "vulnerable to the same method", could someone send samples?

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: