PLATINUM continues to evolve, find ways to maintain invisibility

TN blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/

msft-mmpc

June 7, 2017

Back in April 2016, we released the paper *PLATINUM: Targeted attacks in South and Southeast Asia*, where we detailed the tactics, techniques, and procedures of the PLATINUM activity group.

We described a group that was well-resourced and quickly adopted advanced techniques, such as hot patching to silently inject code into processes. They used *hot patching* even when traditional injection techniques could have been sufficient and less costly to develop.

Since the 2016 publication, Microsoft has come across an evolution of PLATINUM's file-transfer tool, one that uses the Intel® Active Management Technology (AMT) Serial-over-LAN (SOL) channel for communication. This channel works independently of the operating system (OS), rendering any communication over it invisible to firewall and network monitoring applications running on the host device. Until this incident, no malware had been discovered misusing the AMT SOL feature for communication.

Upon discovery of this unique file-transfer tool, Microsoft shared information with Intel, and the two companies collaborated to analyze and better understand the purpose and implementation of the tool. We confirmed that the tool did not expose vulnerabilities in the management technology itself, but rather misused AMT SOL within target networks that have already been compromised to keep communication stealthy and evade security applications.

The updated tool has only been seen in a handful of victim computers within organizational networks in Southeast Asia—PLATINUM is known to customize tools based on the network architecture of targeted organizations. The diagram below represents the file-transfer tool's updated channel and network flow.

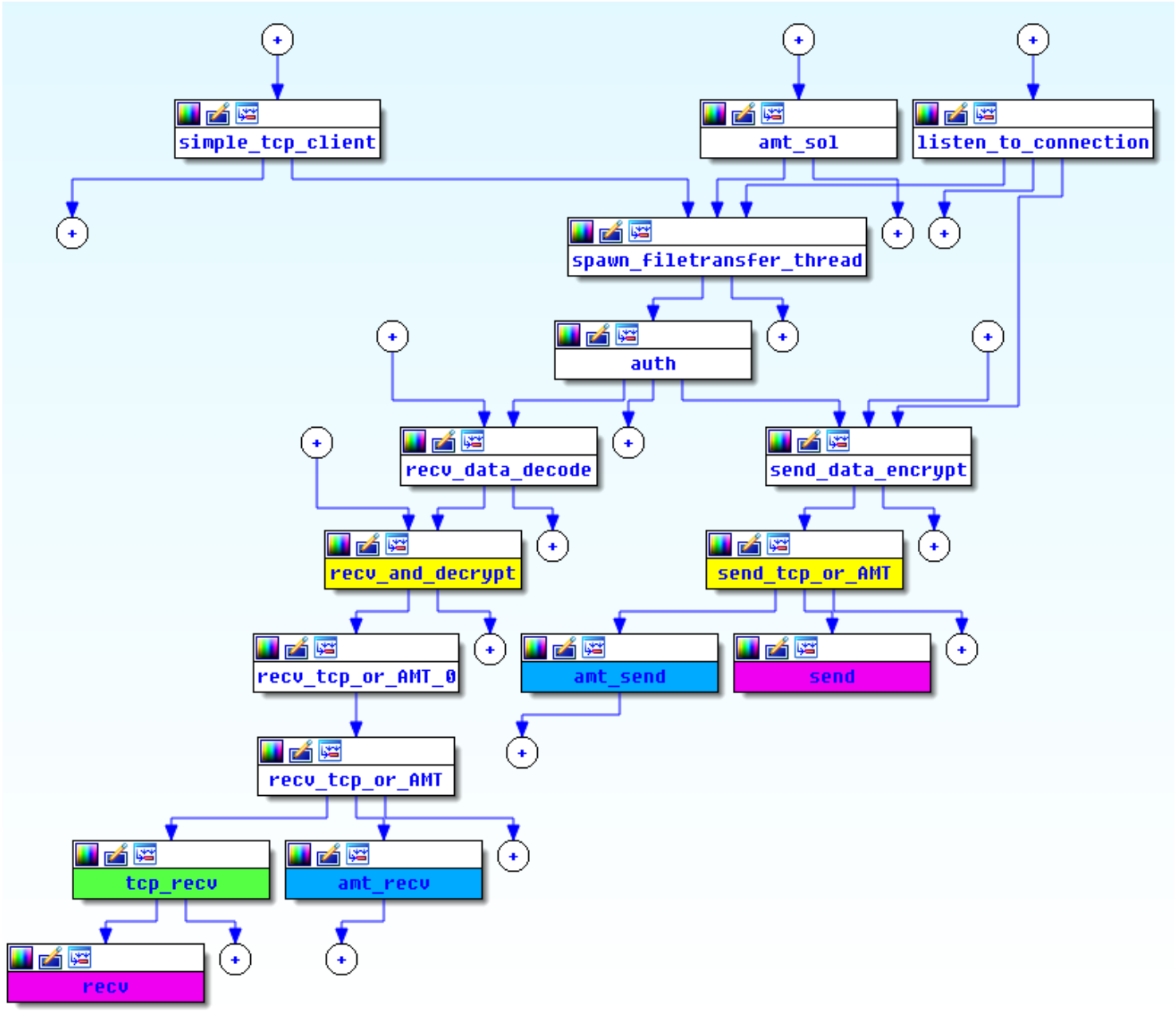

Figure 1. PLATINUM file-transfer tool network flow

The AMT SOL feature is *not* enabled by default and requires administrator privileges to provision for usage on workstations. It is currently unknown if PLATINUM was able to provision workstations to use the feature or piggyback on a previously enabled workstation management feature. In either case, PLATINUM would need to have gained administrative privileges on targeted systems prior to the feature's misuse.

AMT Serial-over-LAN (SOL) communication channel

Active Management Technology (AMT) enables remote management of devices and is provided as a feature of Intel® vPro™ processors and chipsets. AMT runs in the Intel Management Engine (ME), which runs its own operating system to execute on an embedded processor located in the chipset (Platform Controller Hub, PCH). As this embedded processor is separate from the primary Intel processor, it can execute even when the main processor is powered off and is therefore able to provide out-of-band (OOB) remote administration capabilities such as remote power-cycling and keyboard, video, and mouse control (KVM).

AMT has a Serial-over-LAN (SOL) feature that exposes a virtual serial device with a chipset-provided channel over

TCP.

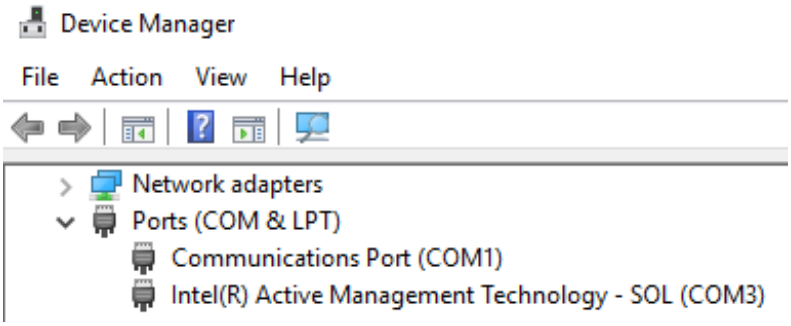

Figure 2. AMT SOL device

This functionality works independently of the device host operating system networking stack—the ME makes use of its own networking stack and has access to the hardware network interface. This means that even if networking is disabled on the host, SOL will still function as long as the device is physically connected to the network.

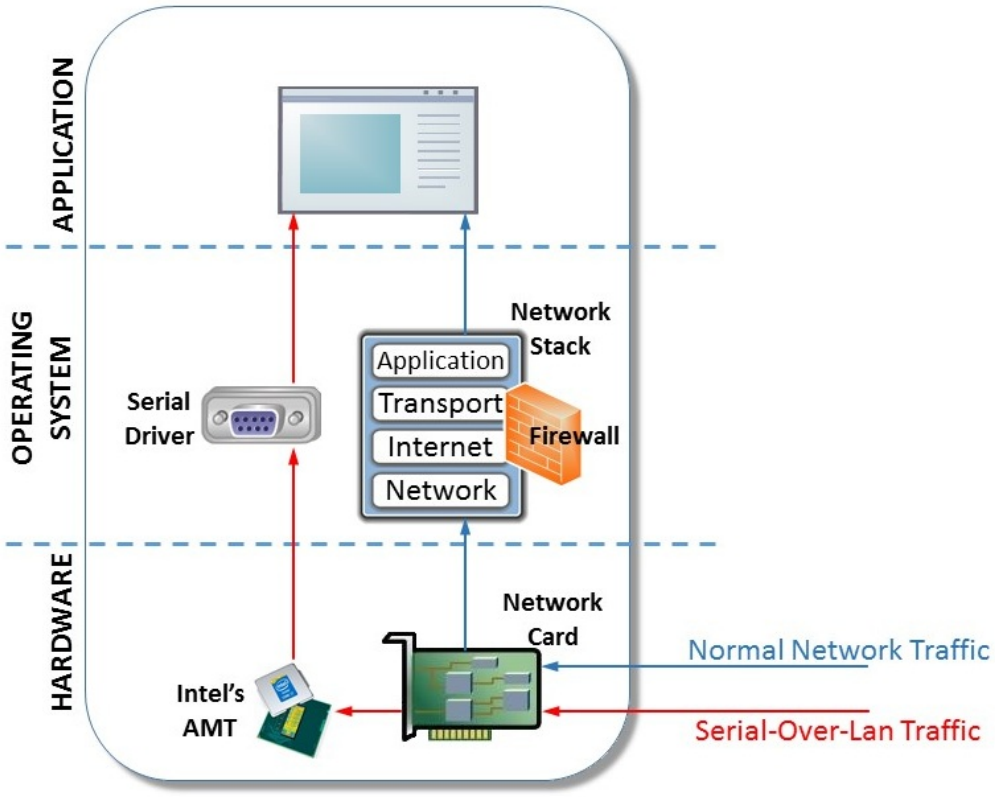

Figure 3. AMT SOL component stack

Furthermore, as the SOL traffic bypasses the host networking stack, it cannot be blocked by firewall applications running on the host device. To enable SOL functionality, the device AMT must be provisioned. Also, establishment of a SOL session requires a username and password—usually selected during device provisioning. The tool would therefore require the relevant credentials to establish such a session.

One possibility is that PLATINUM might have obtained compromised credentials from victim networks. Another possibility is that the targeted systems did not have AMT provisioned and PLATINUM, once they've obtained

administrative privileges on the system, proceeded to provision AMT.

There are several methods for provisioning AMT. The most straightforward is *host-based provisioning (HBP)*, which can be done from within the host Windows OS itself and requires administrator permissions. During the provisioning process, PLATINUM could select whichever username and password they wish. HBP enables access to a subset of AMT functionality, which includes SOL but restricts access to other features such as KVM redirect.

How PLATINUM uses SOL

In the first version of the file-transfer tool, which we described in the original paper, network communication is done over TCP/IP by utilizing the regular network APIs. The presentation layer protocol is straightforward: the buffer is made up of a two-byte header—the indication length—and the Blowfish-encrypted payload data itself.

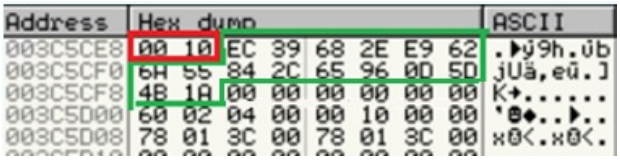

Figure 4. TCP protocol length header and payload

The new SOL protocol within the PLATINUM file-transfer tool makes use of the AMT Technology SDK's Redirection Library API (*imrsdk.dll*). Data transactions are performed by the calls *IMR_SOLSendText()*/*IMR_SOLReceiveText()*, which are analogous to networking *send()* and *recv()* calls. The SOL protocol used is identical to the TCP protocol other than the addition of a variable-length header on the data for error detection. Also, the updated client sends an unencrypted packet with the content "*007*" before authentication.

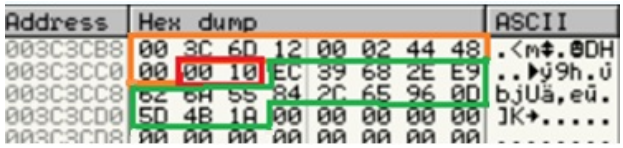

Figure 5. AMT SOL protocol error-detection header, length header, and payload

The new header has various fields to detect possible data corruption errors, including a CRC-16 and a binary index of the bytes having the set of most significant bits (MSB).

```
crc_16_init(&crc16);
crc16_0(&crc16, buf, (unsigned __int16)len);
crc_16_finish(&crc16);
(*new_buffer)->binary_index_of_MSB = 0;
memcpy((unsigned __int8 *)&(*new_buffer)->crc16, &crc16, 2u);
memcpy((unsigned __int8 *)&(*new_buffer)->len_payload, &len, 2u);
memcpy((unsigned __int8 *)&(*new_buffer)->flag, (char *)&a4 + 3, 1u);
memcpy((unsigned __int8 *)(*new_buffer)->binary_index_of_MSB_of_data + padding, buf, (unsigned __int16)len);
i = 1;
do
{
  if ( *(&(*new_buffer)->binary_index_of_MSB + i) > 0x7Fu )
    (*new_buffer)->binary_index_of_MSB |= 1 << (i - 1);
  ++i;
}
while ( i < 6 );
```

Figure 6. Construction of error-detection header

The following video demonstrates how the PLATINUM tool can be used to transfer malware to a computer with AMT provisioned:

Detecting unusual binaries that use AMT

If an attacker who has access to AMT credentials attempts to use the SOL communication channel on a computer running Windows Defender ATP, behavior analytics coupled with machine learning can detect the targeted attack activity. Windows Defender ATP displays an alert similar to the one shown below. Windows Defender ATP can differentiate between legitimate usage of AMT SOL and targeted attacks attempting to use it as a communication channel.

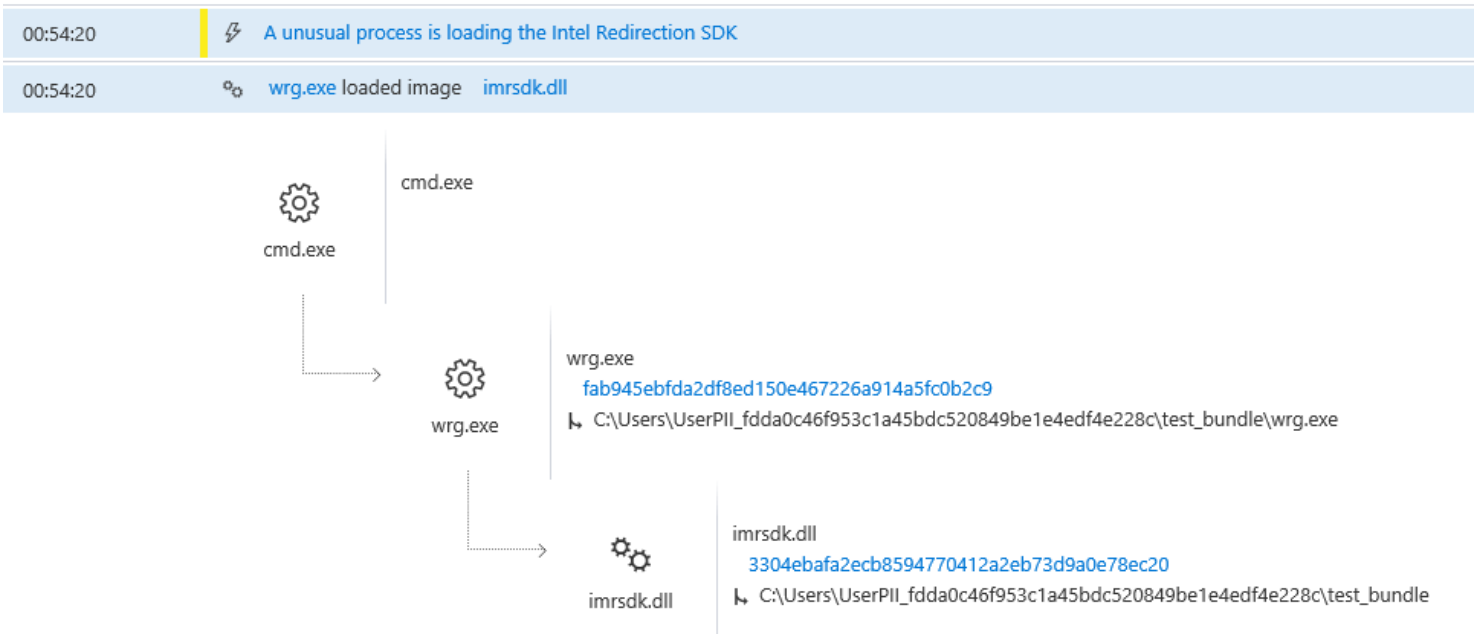

Figure 7. Windows Defender ATP detection of malicious AMT SOL channel activity

The PLATINUM tool is, to our knowledge, the first malware sample observed to misuse chipset features in this way. While the technique used here by PLATINUM is OS independent, Windows Defender ATP can detect and notify network administrators of attempts to leverage the AMT SOL communication channel for unauthorized activity, specifically when used against a computer running Windows.

At Microsoft, we continuously monitor the threat landscape for novel techniques used for malicious purposes. We also constantly build mechanisms that mitigate resulting risks and protect customers. The discovery of this new PLATINUM technique and the development of detection capabilities highlight the work the Windows Defender ATP team does to provide customers greater visibility into suspicious activities transpiring on their networks.

Microsoft reiterates that the PLATINUM tool does not expose flaws in Intel® Active Management Technology (AMT), but uses the technology within an already compromised network to evade security monitoring tools.

David Kaplan, Stefan Sellmer, and Andrea Lelli