Portable Executable File Infecting Malware Is Increasingly Found in OT Networks

mandiant.com/resources/pe-file-infecting-malware-ot

Blog

Ken Proska, Corey Hildebrandt, Daniel Kapellmann Zafra, Nathan Brubaker

Oct 27, 2021

9 mins read

Operational Technology

Threat Research

Malware

While researching files associated with a range of operational technology (OT) original equipment manufacturers (OEM), Mandiant Threat Intelligence uncovered a large number of legitimate portable executable (PE) binaries affected by various types of PE infecting malware. The infected files include binaries associated with programmable logical controllers (PLC), OLE for process control (OPC) communications, human-machine interface (HMI) applications, and other OT functions supported by Windows-based devices at levels 2 and 3 of the Purdue Model.

A PE is a file format developed by Microsoft used for executables (.EXE, .SCR) and dynamic link libraries (.DLL). A PE file infector is a malware family that propagates by appending or wrapping malicious code into other PE files on an infected system. PE infectors are not particularly complex and can be detected by most antivirus products. However, this has not stopped such malware from spreading to OT networks where slight deviations in performance or system conditions may result in adverse outcomes.

For this blog post, we examined 1,200 infected files associated with ten OEMs in a known malware analysis platform from 2010 through 2021. These malicious executables contain infected versions of legitimate PE files as indicated by valid embedded certificates from the vendors. Although we have no indications that this activity is targeting OT systems, our research highlights that actors can often succeed in crossing the OT security perimeter even with simple tactics.

To gain access to comprehensive coverage of OT and IT threat actor activity, check out Mandiant Advantage Free and Fusion cyber threat intelligence offerings.

PE Infecting Malware Is Increasingly Observed in OT Binaries Since 2010

Mandiant hunted for infected samples and uncovered over 1200 infected PEs associated with ten OT OEMs tested in an online malware analysis sandbox from 2010 through 2021. The list of OEMs included Siemens, Emerson, Schneider Electric, Rockwell Automation/Allen Bradley, ABB, Schweitzer Engineering, Honeywell, GE Fanuc, Kepware, and Invensys. In 2010, only three PEs were tested on the platform, but that number increased to 526 PEs in the first six months of 2021 alone. While we are not able to definitively state the reason for this significant increase, there are a few possible explanations.

- Since 2010, awareness of security in OT networks has dramatically increased. As a result, OT security teams increasingly deploy anti-virus measures to Windows-based systems and test more suspicious files, some of which include the identified PE infectors.
- IT-OT convergence has led to increasing connectivity of OT networks, potentially resulting in increased exposure to IT malware like PE infectors.
- Limited use of anti-virus and other security measures in OT has allowed the malware to spread and persist over the last decade.

- OT defenders are increasingly using known malware analysis platforms to review software from Windows-based systems in OT.

Figure 1 shows the upward trend of infected OEM OT executables between 2010 and mid-2021. Mandiant does not have enough information to explain the sudden drop in observed cases during 2019. However, given the observable trend, we believe it may be related to modifications in the malware analysis repository we queried.

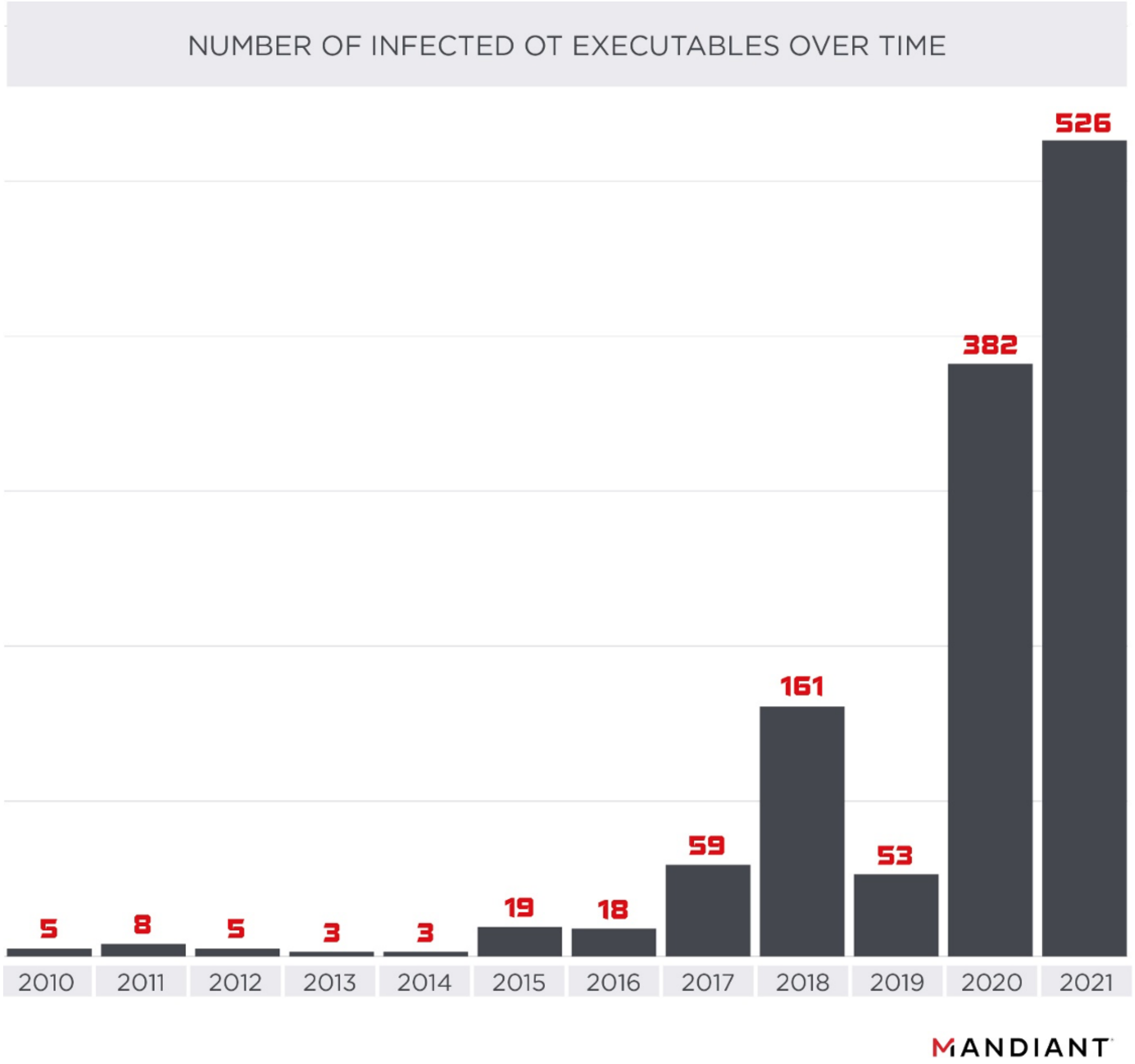


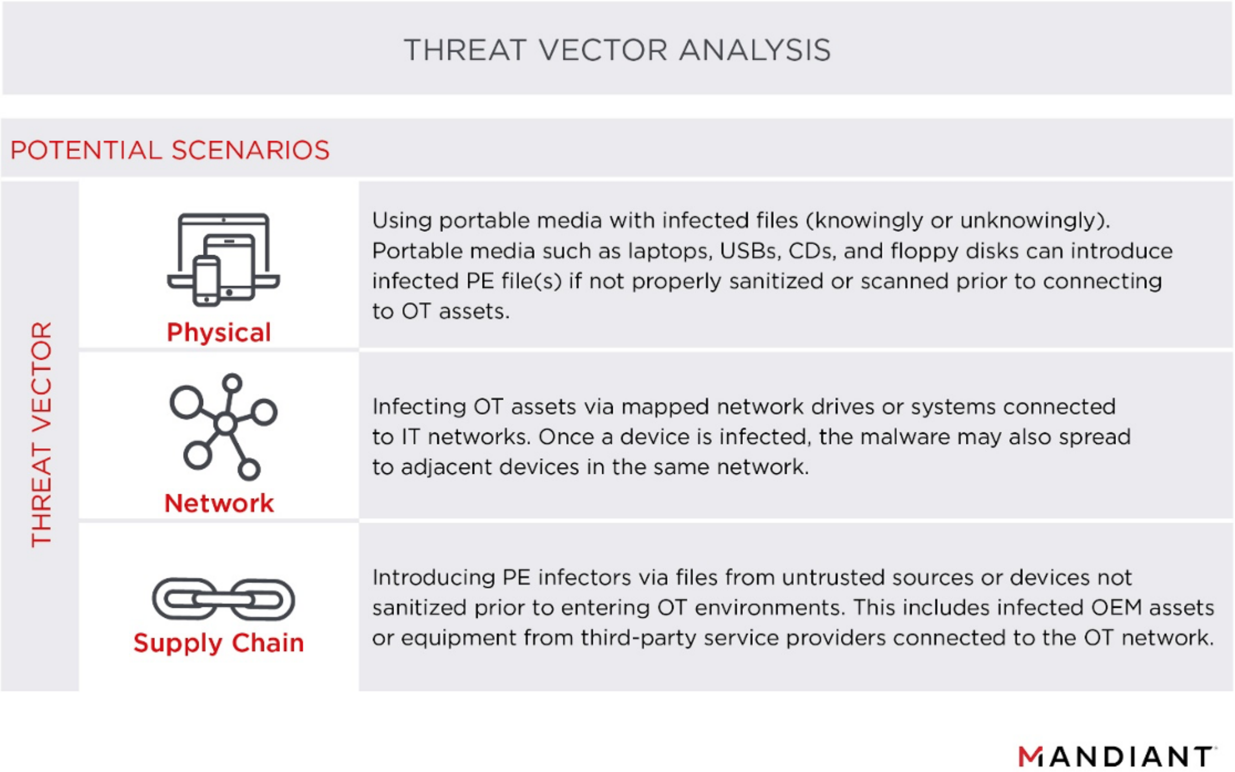
Figure 1: Number of infected OT executables over time

The trend highlighted in Figure 1 is consistent with the fact that the OT security community is relatively new and began to develop mainly after the Stuxnet incident in 2011. We have observed similar growth in other areas, such as information sharing for OT vulnerabilities. We also highlight that the number of infections we present only includes analysis of executables from ten major OEMs in one known malware analysis platform, however, the number of actual infections across the industry is likely much higher.

Download a copy of our sample of infected files. We note that in some cases automated analysis was unable to determine the specific malware and the list may include a small number of other types of malware posing as OT software.

PE Infectors Can Propagate Easily Without Targeting Specific Victims

Mandiant has no information to indicate that any of the PE infectors we uncovered were specifically targeting OT systems. Due to the worm-like nature of many PE infectors, there are multiple scenarios and attack vectors in which OT assets can become infected, most often without being specifically targeted. Table 1 provides a non-exhaustive list of examples.

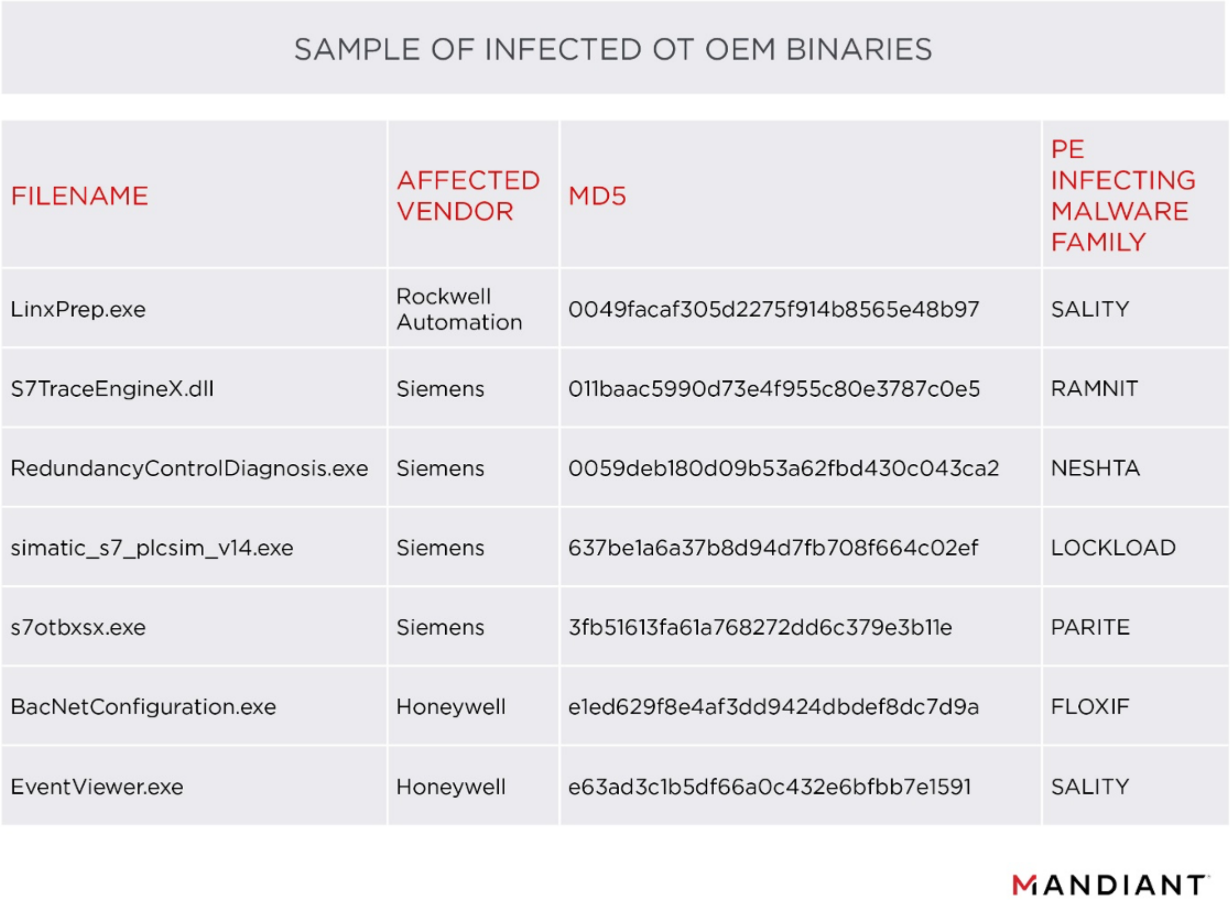


THREAT VECTOR ANALYSIS

THREAT VECTOR		POTENTIAL SCENARIOS
	Physical	Using portable media with infected files (knowingly or unknowingly). Portable media such as laptops, USBs, CDs, and floppy disks can introduce infected PE file(s) if not properly sanitized or scanned prior to connecting to OT assets.
	Network	Infecting OT assets via mapped network drives or systems connected to IT networks. Once a device is infected, the malware may also spread to adjacent devices in the same network.
	Supply Chain	Introducing PE infectors via files from untrusted sources or devices not sanitized prior to entering OT environments. This includes infected OEM assets or equipment from third-party service providers connected to the OT network.

Table 1: Threat vector analysis

PE infectors often propagate by scanning filesystems, memory, local drives, network shares, and portable media for clean PE files and, once located, alter the clean PE by appending malicious code. For example, when the malware finds a file such as “EventViewer.exe”, a legitimate Honeywell software used to view security alarms, it appends itself to the executable but keeps the original name and the program functionality. Procedures used to execute this vary in complexity among different families and variants of PE infectors. Table 2 presents a random sample of infected OT OEM binaries we uncovered.



SAMPLE OF INFECTED OT OEM BINARIES

FILENAME	AFFECTED VENDOR	MD5	PE INFECTING MALWARE FAMILY
LinxPrep.exe	Rockwell Automation	0049facaf305d2275f914b8565e48b97	SALITY
S7TraceEngineX.dll	Siemens	011baac5990d73e4f955c80e3787c0e5	RAMNIT
RedundancyControlDiagnosis.exe	Siemens	0059deb180d09b53a62fbd430c043ca2	NESHTA
simatic_s7_plcsim_v14.exe	Siemens	637be1a6a37b8d94d7fb708f664c02ef	LOCKLOAD
s7otbxsx.exe	Siemens	3fb51613fa61a768272dd6c379e3b11e	PARITE
BacNetConfiguration.exe	Honeywell	e1ed629f8e4af3dd9424dbdef8dc7d9a	FLOXIF
EventViewer.exe	Honeywell	e63ad3c1b5df66a0c432e6bfbb7e1591	SALITY

Table 2: Sample of infected OT OEM binaries

PE infected malware introduced in OT environments can propagate quickly where protection levels are consistent throughout systems and networks. For example, if the initial infection vector is through portable media due to a lack of implementation of scanning and sanitization controls, then asset owners will likely see infections across systems where portable media is shared.

Different PE Infectors Vary in Capabilities

There are multiple types of PE infectors with various capabilities. Our analysis of a subset of identified malicious files indicates the following functions are common across most families:

- Command and Control (C2)

  Provides threat actors with the ability to issue commands, download additional malicious resources, and exfiltrate data from infected systems
- Peer-to-Peer (P2P) Botnet Communication

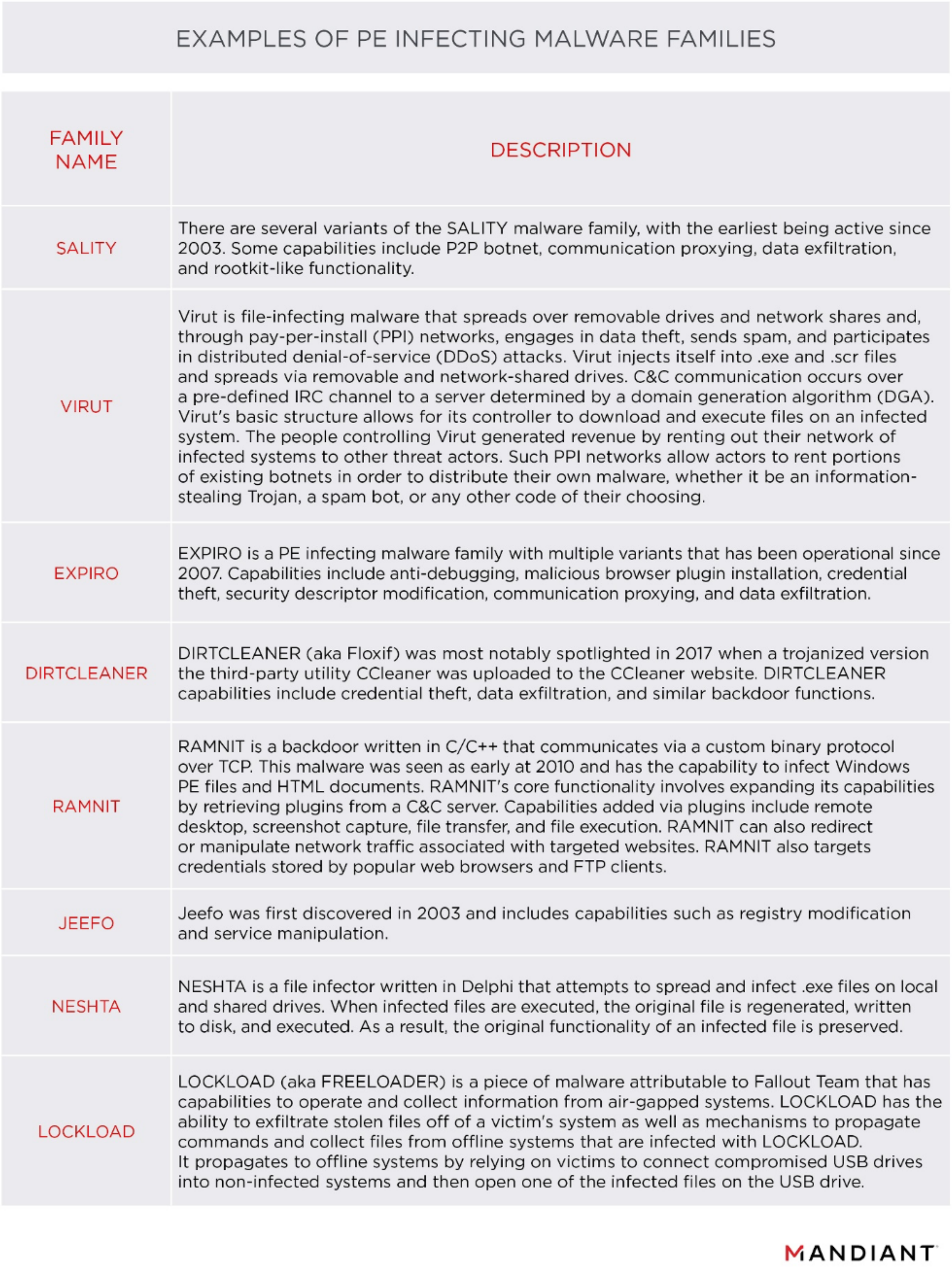
  Ability to send/receive C2 domains/Ips via infected peers
- Anti-Debugging/Anti-VM

  Payload encryption to obscure analysis and detection

- System Modification

  Primarily used to propagate across the system, inject malicious code into processes, alter files across the system, create/delete files, disable security functions, and provide persistence

Table 3 includes a subset of the most observed PE infecting malware families we identified in OT files. Variants may include functionality not mentioned and payloads modified by threat actors.



EXAMPLES OF PE INFECTING MALWARE FAMILIES

FAMILY NAME	DESCRIPTION
SALITY	There are several variants of the SALITY malware family, with the earliest being active since 2003. Some capabilities include P2P botnet, communication proxying, data exfiltration, and rootkit-like functionality.
VIRUT	Virut is file-infecting malware that spreads over removable drives and network shares and, through pay-per-install (PPI) networks, engages in data theft, sends spam, and participates in distributed denial-of-service (DDoS) attacks. Virut injects itself into .exe and .scr files and spreads via removable and network-shared drives. C&C communication occurs over a pre-defined IRC channel to a server determined by a domain generation algorithm (DGA). Virut's basic structure allows for its controller to download and execute files on an infected system. The people controlling Virut generated revenue by renting out their network of infected systems to other threat actors. Such PPI networks allow actors to rent portions of existing botnets in order to distribute their own malware, whether it be an information-stealing Trojan, a spam bot, or any other code of their choosing.
EXPIRO	EXPIRO is a PE infecting malware family with multiple variants that has been operational since 2007. Capabilities include anti-debugging, malicious browser plugin installation, credential theft, security descriptor modification, communication proxying, and data exfiltration.
DIRTCLEANER	DIRTCLEANER (aka Floxif) was most notably spotlighted in 2017 when a trojanized version the third-party utility CCleaner was uploaded to the CCleaner website. DIRTCLEANER capabilities include credential theft, data exfiltration, and similar backdoor functions.
RAMNIT	RAMNIT is a backdoor written in C/C++ that communicates via a custom binary protocol over TCP. This malware was seen as early at 2010 and has the capability to infect Windows PE files and HTML documents. RAMNIT's core functionality involves expanding its capabilities by retrieving plugins from a C&C server. Capabilities added via plugins include remote desktop, screenshot capture, file transfer, and file execution. RAMNIT can also redirect or manipulate network traffic associated with targeted websites. RAMNIT also targets credentials stored by popular web browsers and FTP clients.
JEEFO	Jeefo was first discovered in 2003 and includes capabilities such as registry modification and service manipulation.
NESHTA	NESHTA is a file infector written in Delphi that attempts to spread and infect .exe files on local and shared drives. When infected files are executed, the original file is regenerated, written to disk, and executed. As a result, the original functionality of an infected file is preserved.
LOCKLOAD	LOCKLOAD (aka FREELOADER) is a piece of malware attributable to Fallout Team that has capabilities to operate and collect information from air-gapped systems. LOCKLOAD has the ability to exfiltrate stolen files off of a victim's system as well as mechanisms to propagate commands and collect files from offline systems that are infected with LOCKLOAD. It propagates to offline systems by relying on victims to connect compromised USB drives into non-infected systems and then open one of the infected files on the USB drive.

MANDIANT

Table 3: Examples of PE infecting malware families

PE Infector Outbreaks Can Have Serious Implications for OT Systems

While largely common in IT networks, PE infector outbreaks may have serious implications for OT systems and networks. When PE infectors are not detected and remediated in a timely manner, they can rapidly spread across networks. Widespread infections introduce unexpected conditions to systems and networks where performance and stability are crucial for their intended functions.

- At the network level, systems impacted by PE infecting malware can egress large amounts of erroneous traffic associated with capabilities of the malware, such as C2 beaconing, P2P botnet communication, and file share enumeration. PE infectors may also result in adverse impacts on performance of older networking equipment, which is commonly benchmarked with expected normal conditions through factory acceptance testing (FAT) and site acceptance testing (SAT) by the OEM.
- At the host level, PE infecting malware can cause performance issues for assets. The methods used by the PE infectors to propagate and persist can cause spikes in resource utilization, such as disk I/O, memory, and CPU performance.
    - This can impact legacy systems with limited resources and assets with specific functions such as historians, where disk and memory I/O performance is critical.
    - Binaries used by the OS and OEM software can also become corrupted or degraded as the malware propagates and alters files across the system.

While in most cases, PE infecting malware in OT environments can be considered a nuisance, it highlights the existence of weaknesses that threat actors can take advantage of. Our observations of OT related software executables impacted by PE infecting malware imply that OT systems and networks can be compromised with overly simplistic tactics.

Although the PE infecting malware families we observed were not likely targeting OT systems or networks, more complex malware with similar PE infecting capabilities may be just as effective at penetrating the OT perimeter. One example is the case of LOCKLOAD (aka FREELOADER), a malware family with PE infecting capability which we have observed being used to operate and collect information from air-gapped systems. In addition to its PE infecting ability, LOCKLOAD can exfiltrate stolen files off a victim's system, execute propagate commands and collect files from infected offline systems. It also propagates to offline systems when opening files from compromised USB drives.

Prevention, Detection, and Remediation for PE Infectors in OT Environments

Mandiant provides the following recommendations for prevention, detection, and remediation of PE infectors in OT environments. For support reach out to Mandiant OT Consulting.

Prevention

Defenders should prioritize prevention for PE infecting malware to decrease the risk of infections spreading to critical assets.

- Perform periodic backups for critical assets and ensure backups are tested. The backups should be stored offline and periodically tested.
- Develop policies and procedures for identifying, controlling, and authorizing use of portable media such as laptops, USB, and CDs:
    - Sanitize or scan portable media with up-to-date anti-virus using a heuristics-based engine prior to connecting to OT assets.
    - Evaluate portable media and data entering the OT environment from untrusted sources and have external parties use controlled and authorized portable media.
- Ensure OT assets do not have direct network access or mapped network shares to IT assets unless absolutely required. Properly segment or airgap critical safety assets from larger networks and monitor network traffic for anomalies to and from these assets.
- Monitor vendors' and contractors' use of OT systems, including for example portable media, or work orders.
- Where feasible:
    - Disable USB ports for devices where their use is not needed and, if possible, utilize port-blockers.
    - Install application whitelisting on OT assets or portable media used with OT assets (e.g., maintenance laptops and test equipment).
    - Implement device control on OT assets to ensure only approved portable media is used.

Detection

PE infecting malware and files affected by PE infectors often have high detection rates by anti-virus engines. However, OT systems may be unable to use anti-virus or endpoint protection because of constraints such as service-level agreements (SLA). Defenders should prioritize detection of this threat prior to entering the OT environment. This can be achieved by scanning devices and data brought into the OT environment with updated anti-virus or sanitizing it prior to use.

Detecting the presence of PE infecting malware can be difficult on assets where traditional anti-virus or endpoint protection is not used. This is because the infected PE files may have the ability to run the legitimate code even after being infected, leaving very few user-observable indicators. We suggest defenders review network traffic to and from systems that could be used to support C2 capabilities (e.g., systems at Purdue level 2 and 3). Identifying suspicious beaconing or C2 activity from these assets can also help in identifying infected system in the environment.

Remediation

Remediating an infection caused by PE infecting malware can be complicated due to the self-replicating nature and methods used to propagate and persist throughout a system. Deleting infected files is not recommended as this can cause loss of important files used by the OS or OT applications. Mandiant recommends reverting to known good backups for remediating infected assets. However, reversion to backups requires consideration of the following factors:

- Is there a backup available for the affected asset(s)?
- Were there any changes made to the asset (e.g., configuration, project files, setpoint, tags, etc.) since the last backup was captured?
- What was the infection vector?