# Detecting threat actors in recent German industrial attacks with Windows Defender ATP

**microsoft.com**/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

January 25, 2017


When a Germany-based industrial conglomerate disclosed in December 2016 that it was breached early that year, the breach was revealed to be a professionally run industrial espionage attack. According to the German press, the intruders used the Winnti family of malware as their main implant, giving them persistent access to the conglomerate's network as early as February 2016.

In this blog, we look at the Winnti malware implant as used by two known activity groups BARIUM and LEAD. We look at how these activity groups introduce the implant to various targets and techniques used by Microsoft researchers to track the implant.

To show how this breach and similar breaches can be mitigated, we look at how Windows Defender Advanced Threat Protection (Windows Defender ATP) flags activities associated with BARIUM, LEAD, and other known activity groups and how it provides extensive threat intelligence about these groups. We go through the Winnti implant installation process and explore how Windows Defender ATP can capture such attacker methods and tools and provide visualized contextual information that can aid in actual attack investigation and response. We then discuss how centralized response options, provided as enhancements to Windows Defender ATP with the Windows 10 Creators Update, can be used to quickly stop threats, including stopping command and control (C&C) communication and preventing existing implants from installing additional components or from moving laterally to other computers on the network.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

## Winnti activity groups: BARIUM and LEAD

Microsoft Threat Intelligence associates Winnti with multiple *activity groups*—collections of malware, supporting infrastructure, online personas, victimology, and other attack artifacts that the Microsoft intelligent security graph uses to categorize and attribute threat activity. Microsoft labels activity groups using code names derived from elements in the periodic table. In the case of this malware, the activity groups strongly associated with Winnti are BARIUM and LEAD. But even though they share the use of Winnti, the BARIUM and LEAD activity groups are involved in very different intrusion scenarios.

BARIUM begins its attacks by cultivating relationships with potential victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once BARIUM has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred.

In contrast, LEAD has established a far greater reputation for industrial espionage. In the past few years, LEAD's victims have included:

- Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics
- Pharmaceutical companies
- A company in the chemical industry
- University faculty specializing in aeronautical engineering and research
- A company involved in the design and manufacture of motor vehicles
- A cybersecurity company focusing on protecting industrial control systems

During these intrusions, LEAD's objective was to steal sensitive data, including research materials, process documents, and project plans. LEAD also steals code-signing certificates to sign its malware in subsequent attacks.

In most cases, LEAD's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, LEAD gains

access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.

## Tracking Winnti

Microsoft Analytics shows that Winnti has been used in intrusions carried out throughout Asia, Europe, Oceania, the Middle East, and the United States in the last six months (Figure 1). The most recent series of attacks observed was in December 2016.

*Figure 1. Winnti encounters from July to December 2016*

Although tracking threats like Winnti involves old-fashioned investigative work, Microsoft Threat Intelligence analysts take advantage of machine learning to work at scale. When attackers used Winnti to maintain access to web servers, they hid the implant in plain sight by masquerading it as a trusted, legitimate file. This was the case in two known intrusions in 2015, where attackers named the implant DLL "ASPNET_FILTER.DLL" to disguise it as the DLL for the ASP.NET ISAPI Filter (Table 1). Although there are obvious differences between the legitimate file and the malicious one, filtering out the malicious file would involve going through a data set with noise from millions of possible file names, software publishers, and certificates. Microsoft researchers used a combination of anomaly detection and supervised machine learning to reduce the data set and separate meaningful, malware-related anomalies from benign data.

| | ASPNET_FILTER.dll<br>f00d9d0b64f2467bfdba8510c3d2e68d11a17187<br>Legitimate File | ASPNET_FILTER.dll<br>d740674f54a565ba616c10c8f9c8a4aca9bba82f<br>Winnti DLL |
|---|---|---|
| FileSize | 19,616 | 1,004,124 |
| Image TimeStamp | 2014-02-27 08:13:04 | 0001-01-01 00:02:18 |
| Organization | Microsoft Corporation | - |
| Product | Microsoft® .NET Framework | - |
| Description | Microsoft ASP.NET ISAPI Filter DLL | - |
| Original Name | aspnet_filter.dll | - |
| Version | 2.0.50727.7057 | - |
| Signer | Microsoft Corporation | - |
| Issuer | Microsoft Code Signing PCA | - |

*Table 1. Legitimate ASPNET_FILTER.dll vs. disguised Winnti sample*

## Dealing with Winnti intrusions

Windows Defender ATP helps network security professionals deal with intrusions from activity groups like LEAD and BARIUM in several ways. The following examples were developed using a Winnti installer that was used in attacks in December 2016.

### Alerts for breach activity

Microsoft Threat Intelligence continually tracks activity groups such as LEAD and BARIUM and documents the tactics, techniques, and procedures they employ in their attacks, with a special focus on the tools and infrastructure they use to facilitate those attacks. Windows Defender ATP continuously monitors protected systems for such indicators of hostile activity and alerts security operations center (SOC) personnel to their presence (Figure 2).


*Figure 2. Threat intelligence alert in Windows Defender ATP*

To provide context around such alerts, Windows Defender ATP also features a short summary of the group's history, goals, methods, and tools (Figure 3), with links to extensive documentation for technically minded users.

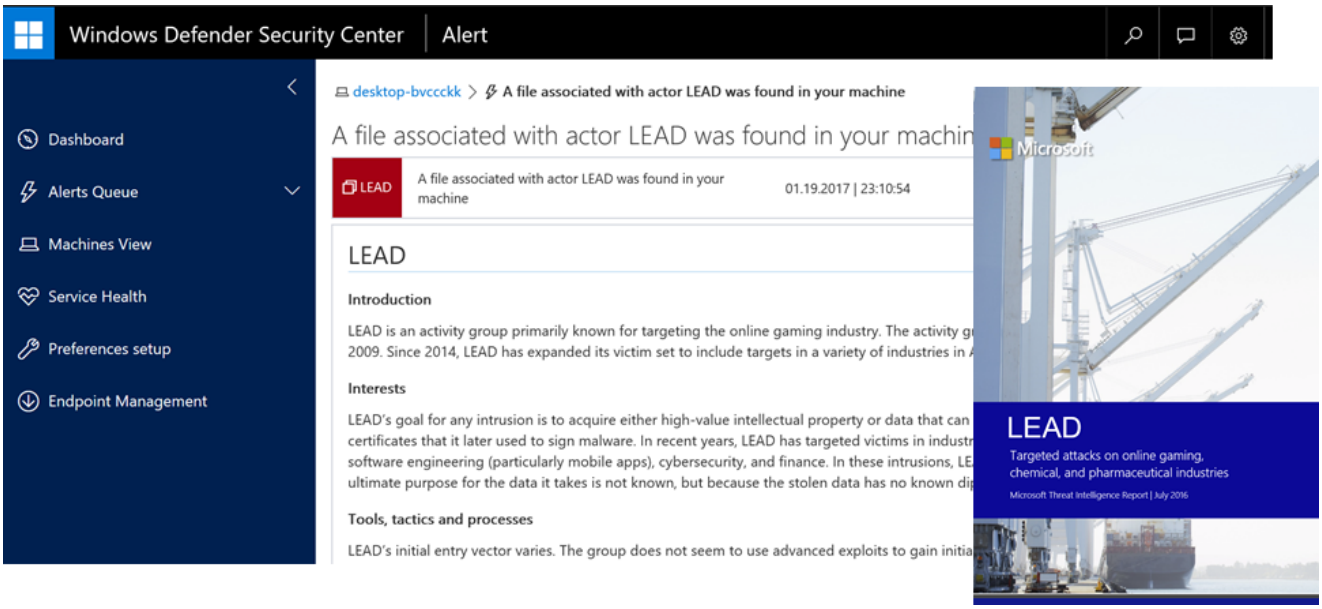


*Figure 3. Lead activity group summary and extensive documentation*

Windows Defender ATP is also capable of detecting previously unknown attacks by monitoring system behavior indicative of hostile activity, including:

- Malware installation, persistence, and activation
- Backdoor command and control
- Credential theft
- Lateral movement to other machines on the network

For example, numerous malware families register themselves as services during installation to guarantee persistence across reboots. A majority of malware that perform this persistence technique modify the necessary registry keys in ways that do not fit the profile of a legitimate program. Winnti is no exception, and so, during Winnti's installation process, Windows Defender ATP is able to raise behavioral alerts (Figure 4).


*Figure 4. Abnormal service creation alert*

To improve coverage while minimizing false positives, Windows Defender ATP uses the intelligent security graph to differentiate between suspicious and benign behavior before generating alerts. It considers the age of the file, its global prevalence, and the presence and validity of a digital signature along with the method of service creation.

## Visualized contextual information

For alerts raised either by specific threat intelligence tied to activity groups or by more generic suspicious behaviors, Windows Defender ATP provides rich, visualized technical context. This visual context enables SOC personnel to investigate alerts with all related artifacts, understand the scope of the breach, and prepare a comprehensive action plan. In the screenshots below, Windows Defender ATP clearly presents the Winnti installation where an installer drops a DLL to disk (Figure 5), loads the DLL using *rundll32* (Figure 6), sets the DLL as a service (Figure 7), and saves a copy of itself in *C:\Windows\Help* (Figure 8).

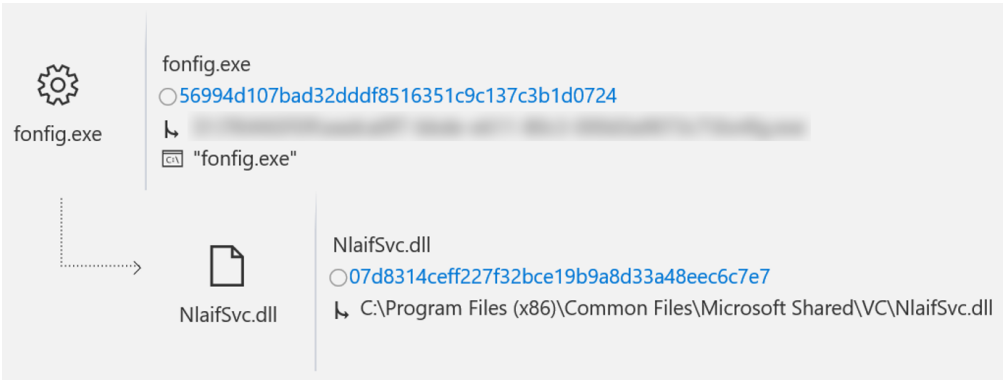


*Figure 5. Winnti installer drops a DLL*

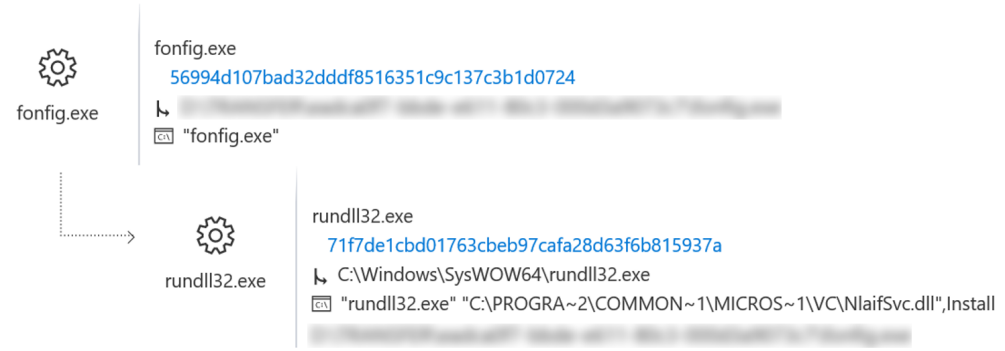


*Figure 6. Winnti installer loads DLL with rundll32*

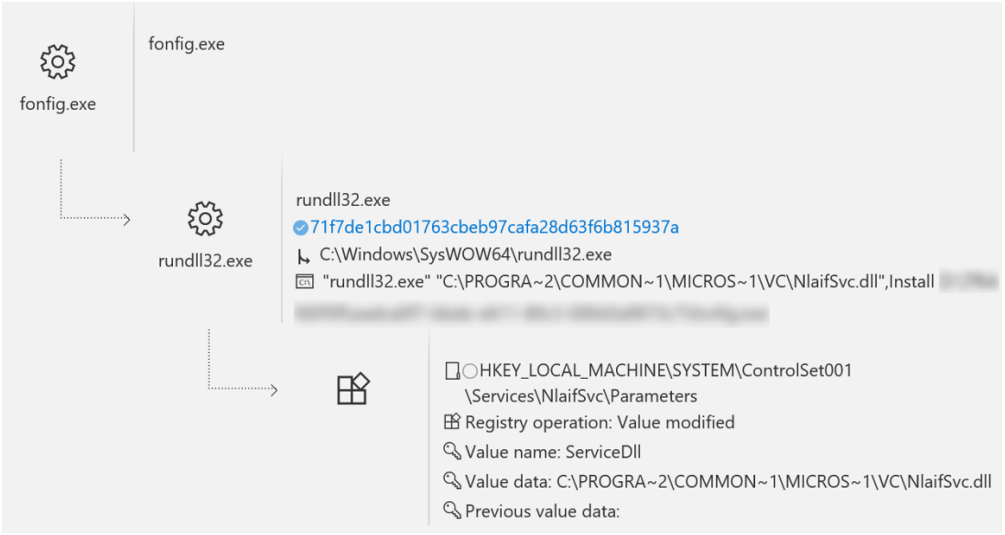

*Figure 7. Winnti sets itself as a service for persistence*

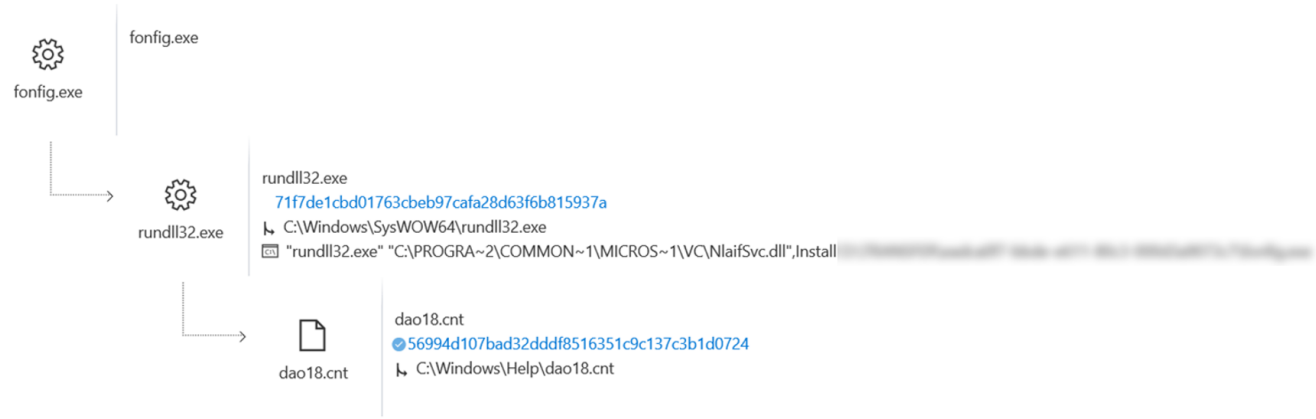


*Figure 8. Installer copied to C:\Windows\Help*

Windows Defender ATP displays these activities as process trees in a machine timeline for the infected computer. Analysts can easily extract detailed information from these trees, such as the implant DLL dropped by the installer, the command used to call rundll32.exe and load the DLL, and the registry modifications that set the DLL as a service. This information can provide an initial means by which to assess the scope of the breach.

## Response options

The Windows 10 Creators Update will bring several enhancements to Windows Defender ATP that will provide SOC personnel with options for immediate mitigation of a detected threat. If an intruder compromises a computer that has been onboarded to Windows Defender ATP, SOC personnel can isolate the computer from the network, blocking command and control of the implant and preventing attackers from installing additional malware and moving laterally to other computers in the network. Meanwhile, connectivity to the Windows Defender ATP service is maintained. While the machine is in isolation, SOC personnel can direct the infected machine to collect live investigation data, such as the DNS cache or security event logs, which they can use to verify alerts, assess the state of the intrusion, and support follow-up actions.

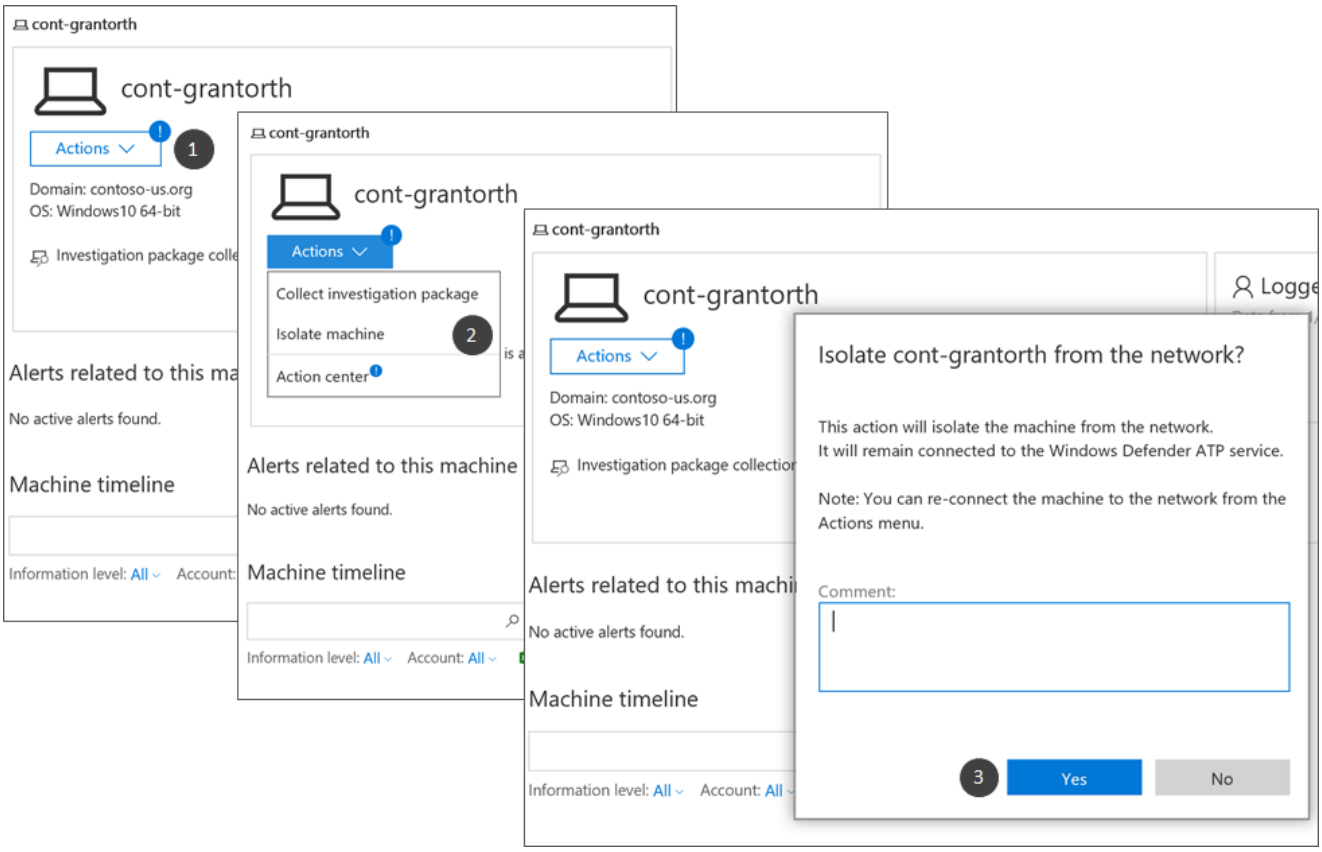


*Figure 9. Response options for the compromised machine*

Another option is to simply halt and quarantine the Winnti implant itself, stopping the intrusion on a single machine. LEAD and BARIUM are not known for large-scale spear-phishing, so it is unlikely that SOC personnel would have to deal with multiple machines having been compromised by these groups at the same time. Nevertheless, Windows Defender ATP also supports blocking the implant across the entire enterprise, stopping large-scale intrusions in the early stages (Figure 10).

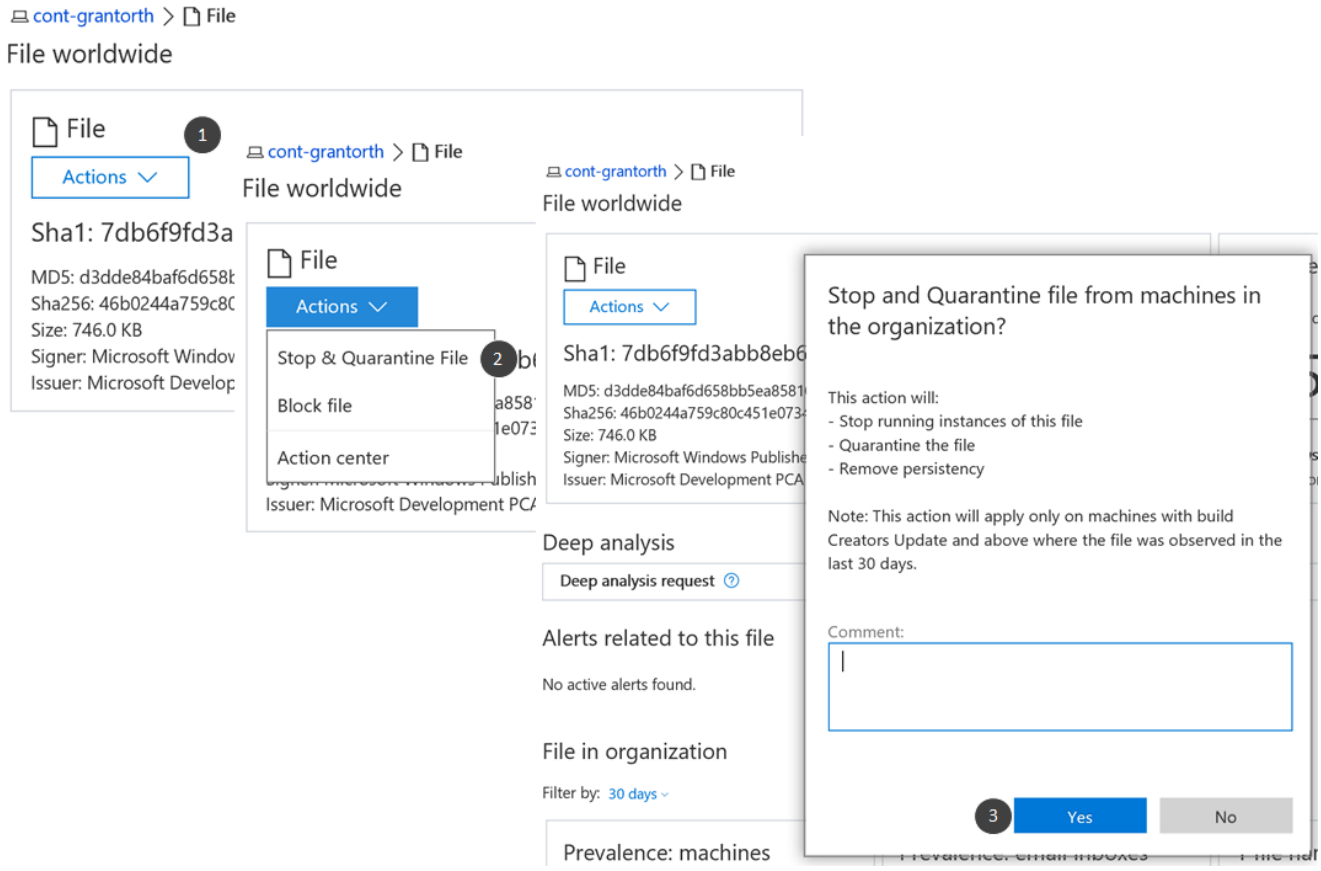


*Figure 10. Response options for the Winnti implant file*

## Conclusion: Shorten breach detection times to reduce impact

According to news reports, the incident affecting the industrial conglomerate may have taken several months to detect and mitigate. The time between the actual breach and its detection may have given attackers enough time to locate sensitive information and exfiltrate this information.

With the enhanced post-breach detection capabilities of Windows Defender ATP, SOC personnel are able to reduce this period to hours or even minutes, significantly lessening the potential impact of persistent attacker access to their network. Windows Defender ATP provides extensive information about activity groups responsible for the attacks, enabling customers to understand aspects of the attack that may not be obtained by network and endpoint sensors, such as common social engineering lures and the regional nature of an attack. With relevant visualized information, analysts are able to study malware behavior on impacted machines, so they can investigate further and plan out their response. And, finally, with the upcoming Creators Update, Windows Defender ATP will provide additional capabilities for detecting threats such as Winnti, as well as centralized response options, such as machine isolation and file blocking, that will enable fast containment of known attack jump off points.

Windows Defender ATP is built into the core of Windows 10 Enterprise and can be **evaluated free of charge**.

*Peter Cap, Mathieu Letourneau, Ben Koehl, and Milad Aslaner*

*This blogpost is also available in German.*

---

## Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.