DATA SHEET

Trellix Intelligent Sandbox

Detect advanced malware

Key benefits

Broad solution integration

- Integration with existing Trellix solutions, third-party email gateways, and other products supporting open standards
- Closes the gap from encounter to containment and protection across the organization
- Streamlines workflows to expedite response and remediation
- Enables automation

Powerful analysis capabilities

- Combines in-depth static code analysis, dynamic analysis, and machine learning for more accurate detection with unparalleled analysis data
- Advanced features support the SOC and enable investigations

Flexible, centralized deployment

- Reduces costs with centralized deployment that supports multiple protocols
- Flexible deployment options support every network

Overview

Trellix Intelligent Sandbox enables your organization to detect advanced, evasive malware and convert threat information into immediate action and protection. Unlike traditional sandboxes, it includes additional inspection capabilities that broaden detection and expose evasive threats.

Tight integration between security solutions—from network and endpoint to investigation—enables instant sharing of threat information across the environment, enhancing protection and investigation. Flexible deployment options support every network.

Our technology has transformed the act of detection by connecting advanced malware analysis capabilities with existing defenses and sharing threat intelligence with the entire IT environment. By sharing threat intelligence across the ecosystem, integrated security solutions can work together to immediately shut down command-and-control communications, quarantine compromised systems, block additional instances of the same or similar threats, assess impact, investigate, and take action.

Intelligent Sandbox: a multifaceted way to detect advanced threats

Intelligent Sandbox detects today's stealthy, zero-day malware with an innovative, layered approach. It combines low-touch analysis engines such as antivirus signatures, reputation, and real-time emulation with dynamic analysis (sandboxing) to analyze actual behavior. Investigation continues with in-depth static code analysis that inspects file attributes and instruction sets to determine intended or evasive behavior and assesses similarity with known malware families. A final step in the analysis, Intelligent Sandbox specifically looks for malicious indicators that have been identified through machine learning via a deep neural network. Combined, this represents the strongest advanced malware security protection on the market and effectively balances the need for both in-depth inspection and performance.

While lower analytical intensity methods such as signatures and real-time emulation benefit performance by catching more easily identified malware, the addition of in-depth static code analysis and insights gained through machine learning to sandboxing broadens detection of highly camouflaged, evasive threats. Malicious indicators that may not execute in a dynamic environment can be identified through unpacking, in-depth static code analysis, and machine learning insights.

Malware writers use packing to change the composition of the code or to hide it in order to evade detection. Most products cannot properly unpack the entire original executable source code for analysis. Intelligent Sandbox includes extensive unpacking capabilities that remove obfuscation, exposing the original executable code. It enables in-depth static code analysis to look beyond high-level file attributes for anomalies, analyzing attributes and instruction sets to determine the intended behavior.

Together, in-depth static code, machine learning, and dynamic analysis provide a complete, detailed evaluation of suspected malware. Unparalleled analysis output produces summary reports that provide broad understanding and action prioritization, and more detailed reports that deliver analyst-grade data on malware.

Enhance protection from the network edge through the endpoint

Tight integration between Intelligent Sandbox and security devices enables integrated security devices to take immediate action when Intelligent Sandbox convicts a file as malicious. This tight and automated integration between detect and protect is critical.

Intelligent Sandbox can integrate in different ways: direct with select security solutions, through Trellix Threat Intelligence Exchange (TIE), or through Trellix Intelligent Sandbox Email Connector. A direct integration enables security solutions to act on files convicted by Intelligent Sandbox. They can immediately incorporate threat intelligence into existing policy enforcement processes and block additional instances of the same or similar files from entering the network.

Intelligent Sandbox convictions appear in the integrated products' logs and dashboards as if the entire analysis had been completed onboard, streamlining workflows and enabling administrators to efficiently manage alerts by working through a single interface.

Integration with TIE extends Intelligent Sandbox capabilities to additional defenses, including the Trellix Endpoint Protection Platform, and enables a broad range of integrated security solutions to access analysis results and indicators of compromise. If a file is convicted by Intelligent Sandbox, TIE immediately publishes threat information via a reputation update to all integrated countermeasures within the organization.

TIE-enabled endpoints can block patient-zero malware installations and provide proactive protection if the file appears in the future. TIE-enabled gateways can prevent the file from entering the organization. Additionally, TIE-enabled endpoints continue to receive file conviction updates when off-network, eliminating blind spots from out-of-band payload delivery.

Intelligent Sandbox Email Connector enables Intelligent Sandbox to receive email attachments for analysis from an email gateway. The solution analyzes files in the attachments and returns a verdict to all active email gateways within the header of the message. The email gateway can then take policy-based action, such as deleting or quarantining the attachment, preventing the malware from infecting and spreading into the internal network.

An offline mode enables email with attachments to be delivered to the end user while being scanned by Intelligent Sandbox. The email gateway does not wait for a verdict on the attachment. Administrators view attachment scanning results through Intelligent Sandbox or TIE. For enhanced detection at the email server, Intelligent Sandbox integrates with Trellix Email Security – Server through TIE.

Threat-sharing to enhance and automate investigations

To investigate and remediate an attack, organizations need comprehensive visibility with actionable intelligence to make better decisions and respond appropriately. Intelligent Sandbox produces in-depth threat intelligence that is easily shared across your entire environment to enhance and automate investigations.

Support for Trellix Data Exchange Layer (DXL) and REST application programming interfaces (APIs) facilitates integrations with other products and widely used threat-sharing standards. These standards include Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII). Integrating them further enables your organization to create, support, and expand a collaborative security ecosystem.

Within a Trellix ecosystem, Trellix Enterprise Security Manager consumes and correlates detailed file reputation and execution events from Intelligent Sandbox and other security systems. In this way, it provides advanced alerting and historic views for enhanced security intelligence, risk prioritization, and real-time situational awareness.

With indicator of compromise data from Intelligent Sandbox, Enterprise Security Manager will look back up to six months to hunt for indications of these artifacts in any network or system data it has retained. It can reveal systems that have previously communicated with newly identified malware sources. Tight integration with the Endpoint Protection Platform, TIE, and Trellix Active Response optimizes security operations response and efficiency. You get improved visibility and can quickly issue new configurations, implement new policies, remove files, and deploy software updates that can proactively mitigate risk.

You can easily take informed action when infected endpoints across the network are automatically identified by Active Response and listed in Intelligent Sandbox reports. Analyst efficiency is increased when these detailed reports are viewed from a single workspace within Active Response.

Integrated solutions

- Trellix Active Response
- Trellix Intelligent Sandbox Email Connector
- Trellix Enterprise Security Manager
- Trellix ePolicy Orchestrator
- Trellix Intrusion Prevention System
- Trellix Threat Intelligence Exchange (TIE)
- Trellix Application Control for Linux
- Trellix Application Control for Windows
- Trellix Endpoint Protection Platform
- Trellix Email Security – Server
- Trellix Endpoint Security for Servers
- Trellix Web Gateway
- Zeek Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)
- STIX (Structured Threat Information eXpression)

Advanced capabilities support investigation

Intelligent Sandbox offers numerous, advanced capabilities, including:

- **Configurable operating system and application support.** Tailors analysis images with select environment variables to validate threats and support investigation.
- **User interactive mode.** Enables analysts to interact directly with malware samples.
- **Extensive unpacking capabilities.** Reduces investigation time from days to minutes.
- **Full logic path.** Supports deeper sample analysis by forcing execution of additional logic paths that remain dormant in typical sandbox environments.
- **Sample submission to multiple virtual environments.** Speeds investigations by determining which environment variables are needed for file execution.
- **Detailed reports.** Provides critical information for investigations, including MITRE ATT&CK mapping, disassembly output, memory dumps, graphical function call diagrams, embedded or dropped file information, user API logs, and PCAP information. Threat timelines help visualize attack execution steps.
- **Zeek Network Security Monitor integration.** By deploying a Zeek sensor to a suspected network segment, you can monitor and capture traffic and forward files to Intelligent Sandbox for inspection.

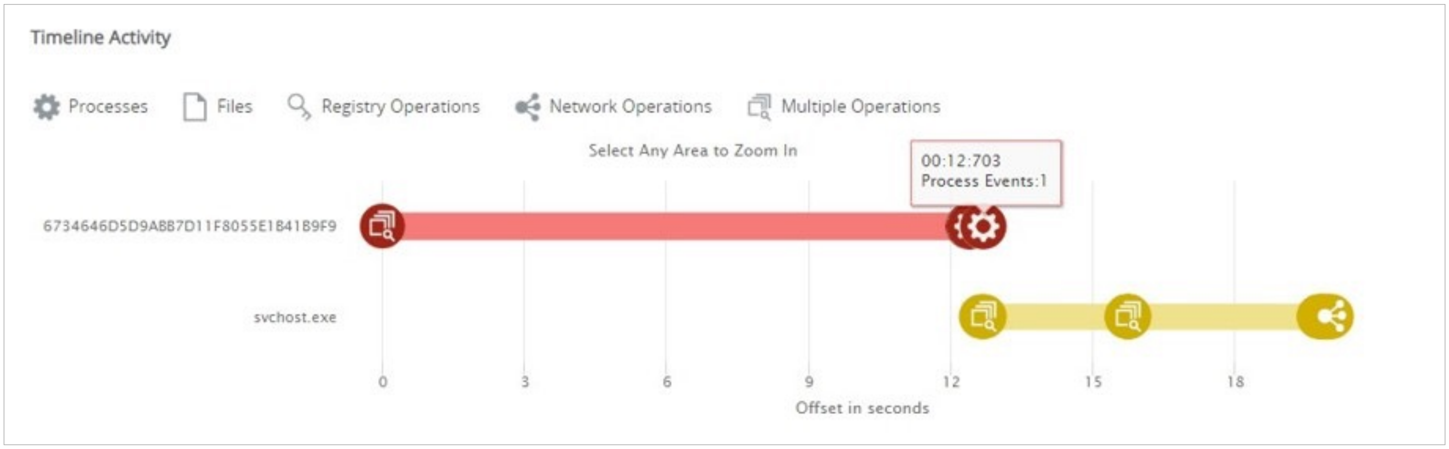
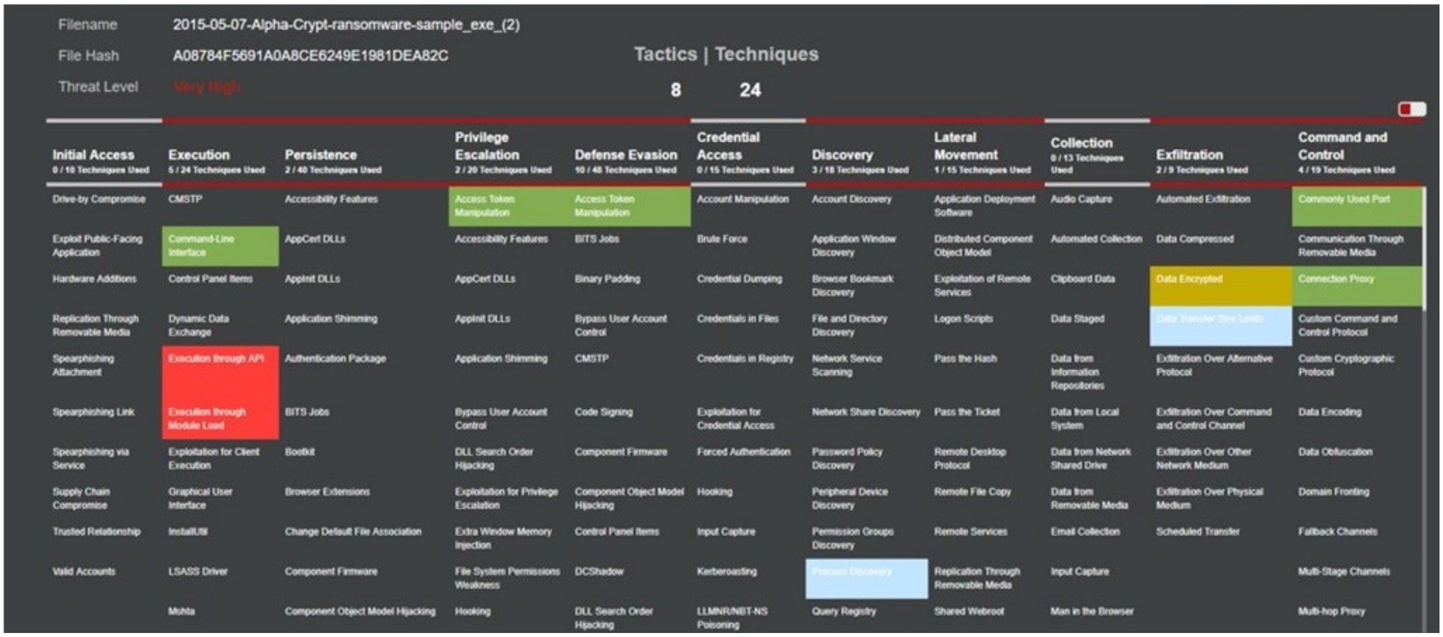


Figure 1. Timeline activity visualizes execution steps of the analyzed threat

Deployment

Flexible advanced threat analysis deployment options support every network. Intelligent Sandbox is available as an on-premises appliance or a virtual form factor, with support for both private and public cloud with availability in the Azure Marketplace.

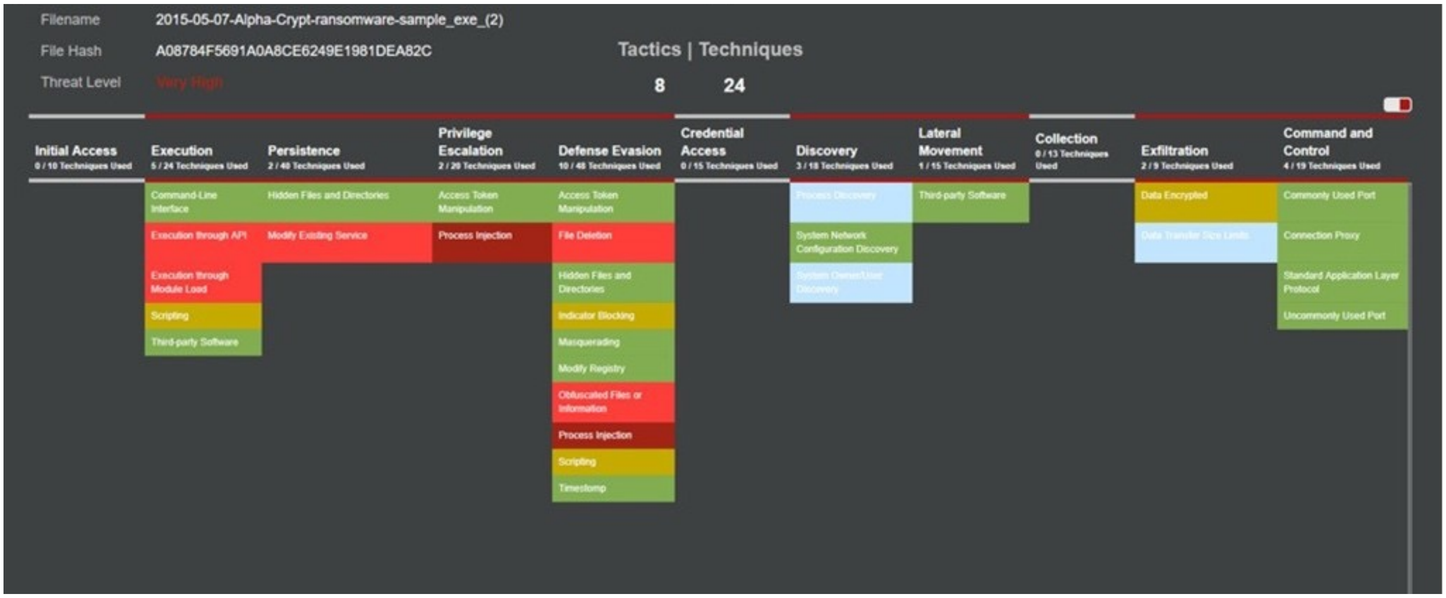


Filename 2015-05-07-Alpha-Crypt-ransomware-sample_exe_(2)
File Hash A08784F5691A0A8CE6249E1981DEA82C
Threat Level Very High

Tactics | Techniques
8 24

Initial Access 0 / 10 Techniques Used	Execution 5 / 24 Techniques Used	Persistence 2 / 40 Techniques Used	Privilege Escalation 2 / 20 Techniques Used	Defense Evasion 10 / 48 Techniques Used	Credential Access 0 / 15 Techniques Used	Discovery 3 / 18 Techniques Used	Lateral Movement 1 / 15 Techniques Used	Collection 0 / 13 Techniques Used	Exfiltration 2 / 9 Techniques Used	Command and Control 4 / 19 Techniques Used
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy

Figure 2. Results map to MITRE ATT&CK framework



Filename 2015-05-07-Alpha-Crypt-ransomware-sample_exe_(2)
File Hash A08784F5691A0A8CE6249E1981DEA82C
Threat Level Very High

Tactics | Techniques
8 24

Initial Access 0 / 10 Techniques Used	Execution 5 / 24 Techniques Used	Persistence 2 / 40 Techniques Used	Privilege Escalation 2 / 20 Techniques Used	Defense Evasion 10 / 48 Techniques Used	Credential Access 0 / 15 Techniques Used	Discovery 3 / 18 Techniques Used	Lateral Movement 1 / 15 Techniques Used	Collection 0 / 13 Techniques Used	Exfiltration 2 / 9 Techniques Used	Command and Control 4 / 19 Techniques Used
	Command-Line Interface	Hidden Files and Directories	Access Token Manipulation	Access Token Manipulation		Process Discovery	Third-party Software		Data Encrypted	Commonly Used Port
	Execution through API	Modify Existing Service	Process Injection	File Deletion		System Network Configuration Discovery			Data Transfer Size Limits	Connection Proxy
	Execution through Module Load			Hidden Files and Directories		System Owner/User Discovery				Standard Application Layer Protocol
	Scripting			Indicator Blocking						Uncommonly Used Port
	Third-party Software			Masquerading						
				Modify Registry						
				Obfuscated Files or Information						
				Process Injection						
				Scripting						
				Timestomp						

Figure 3. A filtered view of the results displayed in Figure 2 focuses report on identified techniques

Table 1. Trellix Intelligent Sandbox specifications

Physical form factor	ATD-3200 1U Rack-mount	ATD-6200 1U Rack-mount
Virtual form factor	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V Windows Server 2012 R2, Windows Server 2016	
Detection		
File sample types supported	PE files, Adobe files, Microsoft Office Suite files, image files, Archives, Java, Android Application Package, URLs	
Analysis methods	Trellix Antimalware, GTI reputation: file/URL/IP, Gateway Antimalware (emulation and behavioral analysis), dynamic analysis (sandboxing), in-depth code analysis, custom YARA rules, machine learning	
Supported OS	Windows 10 (64-bit), Windows 8.1 (64-bit), Windows 8 (32-bit/64-bit), Windows 7 (32-bit/64-bit), Windows XP (32-bit/64-bit), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android	
Output formats	STIX, OpenIOC, XML, JSON, HTML, PDF, text	
Submission methods	Point product integrations, RESTful APIs, manual submission, and Intelligent Sandbox Email Connector (SMTP)	

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.