Company Profile

FFRI Security, Inc.
https://www.ffri.jp/en/index.htm

Ver2.00.09

Company Profile

Company Name: FFRI Security, Inc.
(TSE Market of High-Growth and Emerging Stocks: 3692)

President and CEO : Yuji, Ukai

Address : 2F Shin-Tokyo Building,
3-3-1, Marunouchi, Chiyoda-ku, Tokyo, JAPAN, 100-0005

Date of Establishment : July 3, 2007

Capital : ¥286,136,500 (as of March 31, 2019)

Scope of business

1. Computer security research, consulting, information provision, and education
2. Network system research, consulting, information provision, and education
3. Computer software and computer program planning, development, sales, leasing, maintenance, management, and operation, and the acquisition, transfer, lending, and management of related property rights such as copyrights, publishing rights, patent rights, utility model rights, trademark a rights, design rights
4. All duties related to the above businesses

Business Overview

Seed based R&D in Cyber Security

- Research regarding security vulnerabilities used for targeted attacks, etc. and development of countermeasure technology
  Track record of discovering more than 100 critical vulnerabilities (most in Japan)
  Research regarding targeted attack malware and development of countermeasure technology
- Numerous announcements of research results regarding malware security measures in recent years, such as for targeted attacks
- Built-in security
  Numerous announcements of research results regarding security vuln
  threat analyses of built-in systems

Products

- Vulnerability attack protection software
- Targeted Attack countermeasure software
- Automated malware analysis tool
- MITB Attack countermeasure software
- Embedded device security inspection tool
- P2P system security

Services

- Targeted attack malware inspection analysis
- Smart device security inspections
- Security measures consulting
- Contracted research and development
- Black URL provision service
- Security technician training

Research regarding security vulnerabilities and development of countermeasure technology

Track record of discovering more than 100 critical vulnerabilities (most in Japan)

Track record of research in security vulnerability countermeasures

- Announcement of research regarding vulnerability analysis at various international conferences, such as BlackHat USA/Japan, RSA Conference, and CanSecWest
- Announcement of various research results at http://www.ffri.jp/research/index.htm

Track record of discovering security vulnerabilities

Track record of discovering more than 100 critical vulnerabilities

Examples: Microsoft Windows (LSASS vulnerability, wkssvc vulnerability, animated cursor vulnerability, GDI vulnerability, Office products, Internet Explorer, etc.), Winny, Ichitaro, QuickTime, Realplayer, etc.

Featured in various articles, magazines, newspapers, and on NHK news

Example: Discovery of vulnerability in IPv6 stack (included standard in Windows)

Date reported: March 24, 2010/Date published: August 11, 2010

Other

- First in the world to demonstrate the possibility of Windows 9x system stability
- Track record of numerous research announcements in Japan

http://www.ffri.jp/research/index.htm

Research regarding malware and development of countermeasure technology

Numerous announcements of research results regarding malware security measures in recent years, such as for targeted attacks

Contracted by the Information-technology Promotion Agency (IPA): Research regarding targeted attacks in recent years

Comprehensive reverse engineering and behavioral analysis was performed on all codes from several samples regarding malware, vulnerability exploitation techniques, and targeted attacks in recent years.The countermeasures are presented.

http://www.ipa.go.jp/security/fy19/reports/sequential/index.html

Research Results announced at international conferences and in the media

Examples:

"Facts Discovered from an Analysis of Targeted Attack Malware -- Yuji Ukai, FFRI" (builder)
http://builder.japan.zdnet.com/news/story/0,3800079086,20367832,00.htm

Research announcement by FFRI engineers at MWS 2014 (Asahi Shinbun DIGITAL)
http://www.asahi.com/and_M/information/pressrelease/Cdpress000101109.html

SLIME: Automated Anti-sandboxing disarmament system (Black Hat Asia)
https://www.blackhat.com/asia-15/briefings.html#slime-automated-anti-sandboxing-disarmament-system

FREEZE DRYING FOR CAPTURING ENVIRONMENT SENSITIVE MALWARE ALIVE (Black Hat Europe)
https://www.blackhat.com/eu-14/briefings.html#freeze-drying-for-capturing-environment-sensitive-malware-alive

TENTACLE: Envirnment Sensitive Malware Palpation (Pacsec 2014)
http://www.asahi.com/and_M/information/pressrelease/Cdpress000102746.html

Built-In Security

Numerous announcements of research results regarding security vulnerability threat analyses of built-in systems

Private built-in security measures promoted by IPA

Private built-in security measures are promoted by IPA.

"New-Generation Information Security Research and Development Projects" by the Ministry of Economy, Trade, and Industry

Research conducted regarding automatic detection technology for unknown vulnerabilities in devices other than computers, such as information appliances, smart grids, and mobile devices.

Numerous announcements regarding IoT security threat analysis

Examples:

"A security assessment study and trial of TriCore-powered automotive ECU" (Code Blue)
http://www.ffri.jp/assets/files/research/research_papers/Code_Blue_Tricore_assessment_slides_ja.pdf

"How Security Broken?" (PacSec2011)
http://www.ffri.jp/assets/files/research/research_papers/how-security-broken-pacsec2011.ja.pdf

"Yet Another Android Rootkit - /protecting/system/is/not/enough" (Black Hat Abu Dahi 2011)
http://www.ffri.jp/assets/files/research/research_papers/yet-another-android-rootkit.pdf

"Android: Technical Design Issues" (Internet Week 2011)
http://www.ffri.jp/assets/files/research/research_papers/InternetWeek2011_s10-02.pdf

"Windows Phone 7 Internals and Exploitability" (Black Hat USA 2012)
http://www.ffri.jp/assets/files/research/research_papers/wp7-internals-and-exploitability.pdf

Other

Conducted numerous analyses of threats to automotive systems and diagnoses of vulnerabilities in routers, network devices, etc.

Products, Services Lineup

- Corporate -

Targeted Attack Protection

Yarai

Protection against targeted attack malware, known malware, known and unknown security vulnerability attacks, without reliance on patterns.

Targeted Attack Malware Inspection Service

Targeted Attack Malware Inspection Service

Investigation for invasion by targeted attack malware. Analysis of malware and actual damage. Support for reactive measures, including measure planning and external reporting.

Automatic Malware Analysis Tool

Yarai Analyzer
Automated Malware Analysis System

Useful in a variety of malware analysis scenarios, such as inspection for malware infection before software products are shipped and initial analysis of malware damage.

yarai Analyzer Professional
Automated Malware Analysis System

In addition to the functions provided in FFR yarai analyzer, FFR yarai analyzer Professional allows automatic extraction and reporting of more advanced level of information.

Products, Services Lineup

- Personal / SOHO -

Security Protection for Personal and SOHO Environments

Yarai Home and Business Edition

New-generation security software for protection against malicious attackers with a multi-faceted approach.

- Personal -

Security Protection for Personal Environments (Smartphones)

FFRI Secure Application Checker

Security application that can easily diagnose vulnerabilities in applications running on Android smartphones and tablets.

Products, Services Lineup

Security Inspection of IoT Devices

IoT device and system security countermeasure support service

Our research team, which has conducted numerous security threat analyses and published international research results, analyzes security threats to IoT devices and systems before they are shipped, and supports countermeasures.

Security Consulting Service

Prime Analysis

Provision of consulting services for APT malware investigation, Android device security analysis, vulnerability threat analysis, patch analysis, malware analysis, emergency briefings, etc.

List of Risky URLs that Distribute Malware

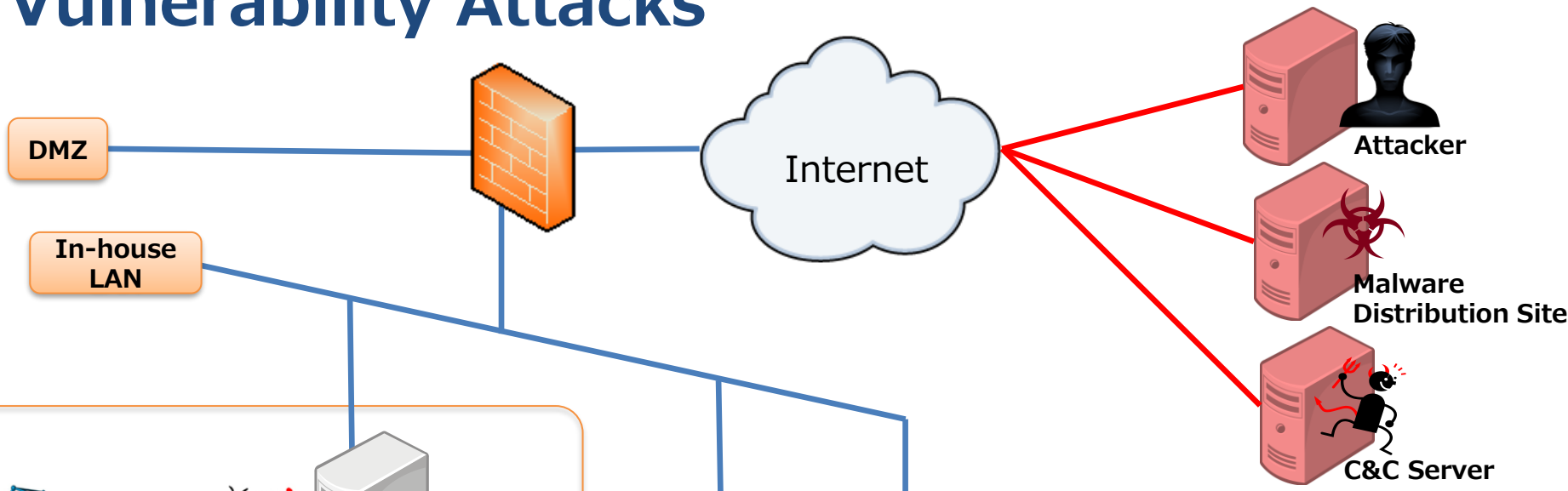
BlackURL

Information is provided regarding risky URLs extracted from malware samples obtained with our malware capture system.

Other service achievements

業種	カテゴリ	内容
Government Agency	Entrusted development	Development of additional functions for anti-cyber attack products and porting to other operating systems
	Education/Training	Malware dynamic analysis training
		Malware static analysis training
	Surveys and research	Creating a system to analyze malware connections
		Research and development on inspection technology for threats to control systems
Telecommunications	Education/Training	Education and training for security engineer development
	Surveys and research	Research and evaluation support for security mechanisms
Industrial Infrastructure/Services	Education/Training	Support for training of security engineers for control systems
	Surveys and research	Malware research for control systems
		Threat analysis for control systems
		Survey of fuzzing methods for control systems
	Investigation/Diagnosis	Support for creating a secure development guide for Android applications
		Testing network devices for security features
Automobile	Investigation/Diagnosis	Consulting on secure development
		Consulting on testing methods for ECUs
		Penetration testing for IVI devices on complete vehicles
	Surveys and research	Assessment of requirements specifications

Security Solutions for Malware and Vulnerability Attacks



Yarai Analyzer
Automated Malware Analysis System

Understand Damage due to Targeted Attack Malware
In addition to initial malware analysis, this tool uses our "targeted attack malware inspection service" to visualize a detailed range of effect and provide support for countermeasures.

Yarai

Release from Operational Load for Endpoint Security

- Use of 5 heuristic detection engines allows protection from unknown attacks without relying on pattern files.
- A secure environment can be maintained even in a closed environment, because detection is not dependent on pattern files.
- Generic mechanisms can be used to protect against arbitrary code execution vulnerability attacks, and therefore the frequency of security patches can be reduced.

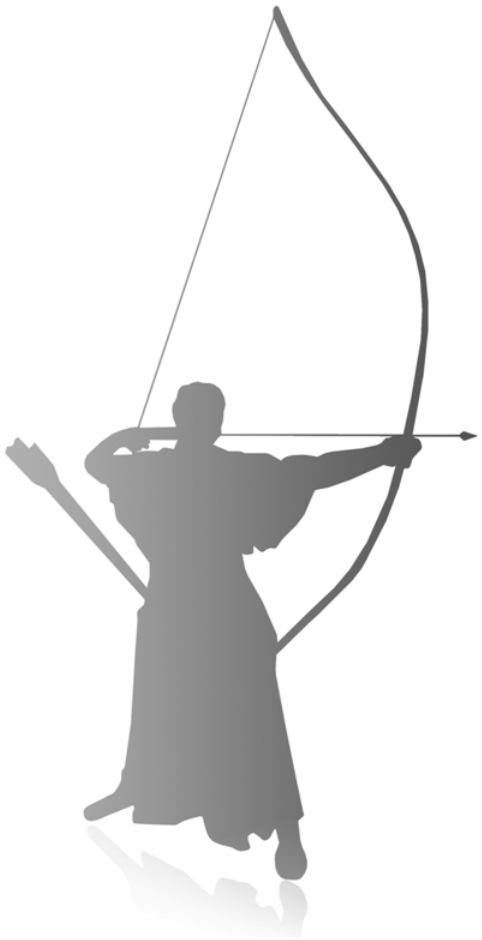
Next-Generation Endpoint Security

FFRI yarai

FFRI Security, Inc.
https://www.ffri.jp/en/index.htm

Ver 3.00.07

Requirements To Protect From Malicious Programs



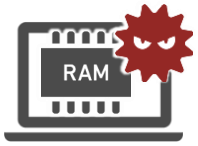
No Dependent on Signatures

Progressive heuristic technology using proactive detection logic without depending on signatures

Behavioral Detection

Detect malware by determining its malicious characteristics and behaviors

Fileless Malware Protection



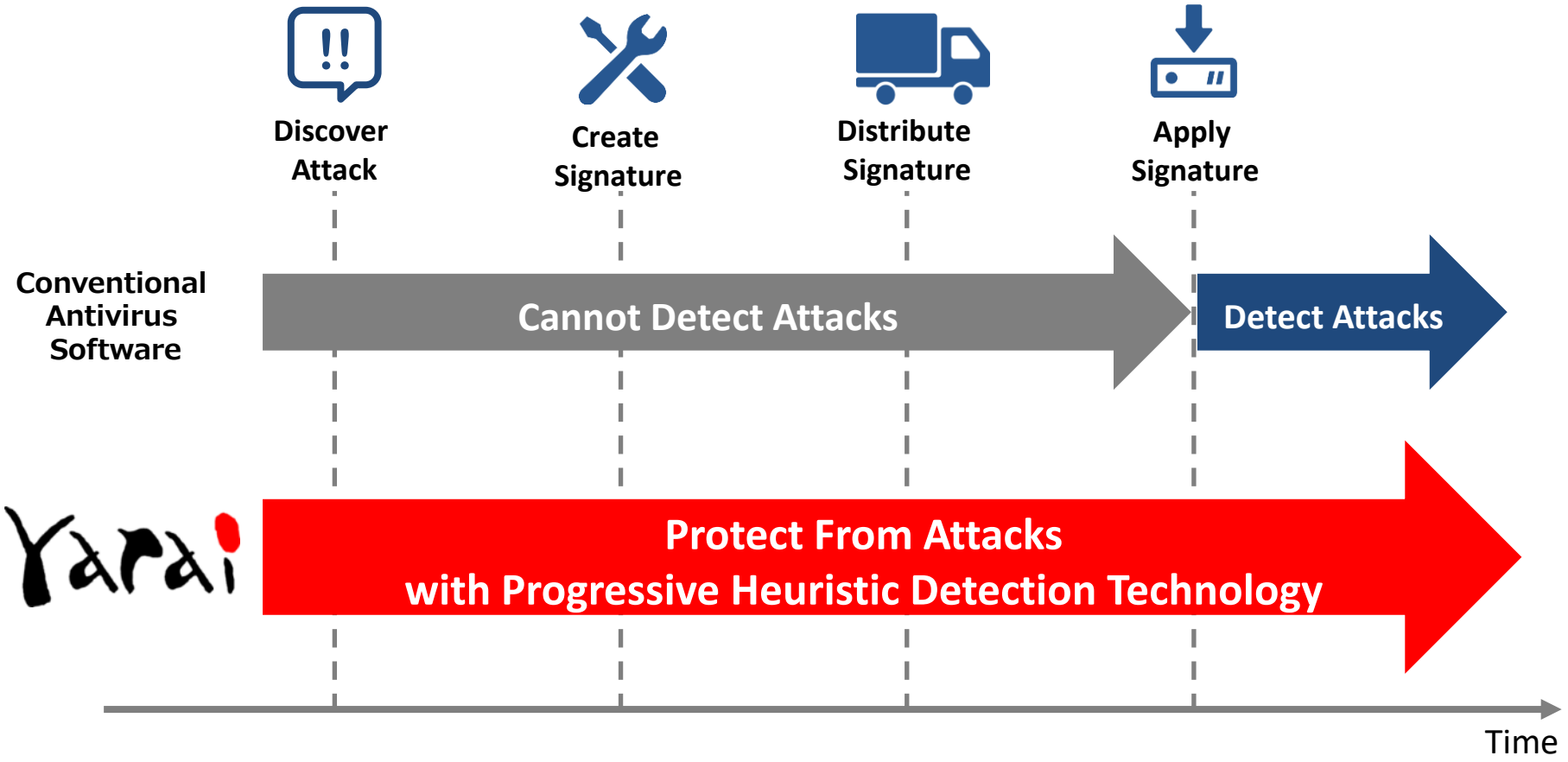
Block fileless malware such as malware using a script file at each phase of an attack

Multi-Layer Protection

Multi-layer endpoint protection with the combination of 5 protection engines to protect from known threats

Limitation With Signature Based Protection

Signature based protection requires lead time before detecting attacks



Five Behavioral Detection Engines of FFRI yarai

ZDP Engine
(Dynamic Analysis)

Protects against virus attacks that target known and unknown vulnerabilities such as attacks when viewing emails or Web pages.
Protects against arbitrary code execution vulnerability attacks by use of our original API-NX technology (Patent No. 4572259).

Static Analysis Engine
(Static Analysis)

Analysis performed without program operation.
Detection is performed by using N-Static Analysis that incorporates numerous analysis methods including PE Structure Analysis, Linker Analysis, Packer Analysis, and Speculated Operation Analysis.

Sandbox Engine
(Semi-Dynamic Analysis)

Runs programs on a virtual environment that includes a virtual CPU, virtual memory and virtual Windows subsystems.
Detection is based on a combination of commands based from our unique U-Sandbox Detection Logic.

HIPS Engine
(Dynamic Analysis)

Monitors the behavior of currently running programs.
Our unique D-HIPS Logic detects behavior such as program intrusion, unusual network access, keylogger and backdoor access behavior.

Machine Learning Engine
(Dynamic Analysis)

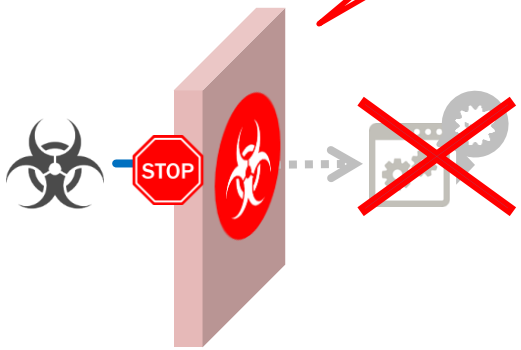
Monitors running programs based on big data related to malware that has been captured by FFRI Security.
Behavioral characteristics in big data are extracted to detect malicious behavior in systems by using machine learning to analyze such characteristics.

Behavioral Detection

Provide real-time monitoring for unauthorized access and writing by malicious programs without depending on signatures to stop execution

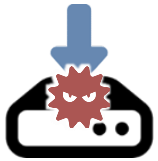
Protect Application From "Vulnerability Attacks"

Block vulnerability attacks (memory corruption attacks) and prevent arbitrary code executions and program executions



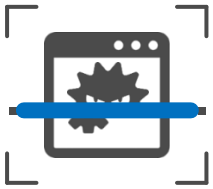
ZDP Engine

Block Malware "Intrusions"



Prevent program executions by statically analyzing the program architecture and detecting malware affecting OS, memory and registry

Prevent program executions by executing the program on the virtual environment and detecting malware affecting OS, memory and registry



Static Analysis Engine

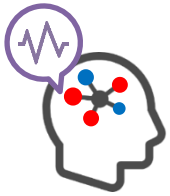
Sandbox Engine

Block Malware "Activities"

Monitor behaviors of executing programs and block execution in case finding malicious access or writing to OS, memory or registry

Monitor behaviors of executing programs and block execution in case finding malicious access or writing to OS, memory or registry

HIPS Engine



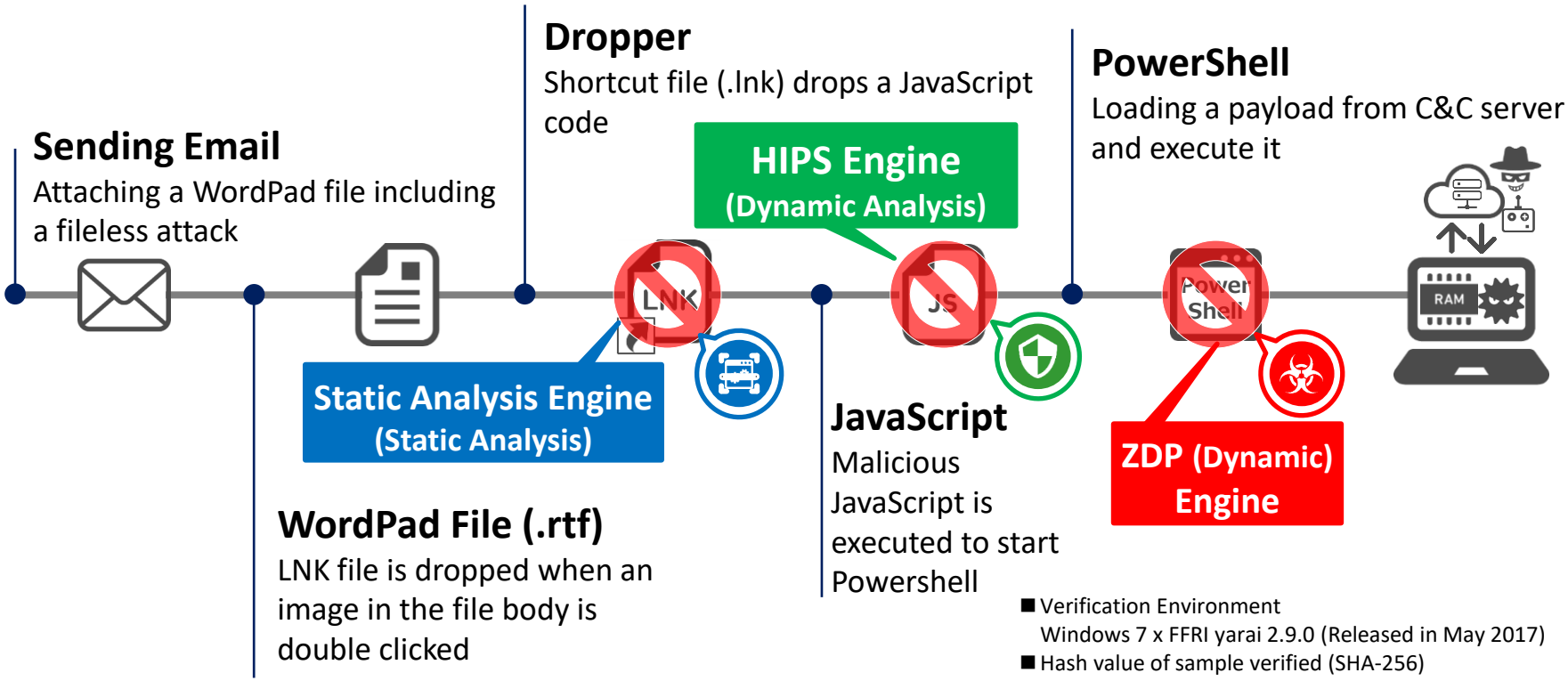
Machine Learning Engine

Fileless Malware Protection

Detect fileless malware such as malware using scripts for attack and prevent the execution

Fileless Malware Attack
Attack executed on memory without using an executable file

Fileless Malware Attack Targeting Restaurants All Over The United States (June 2017)

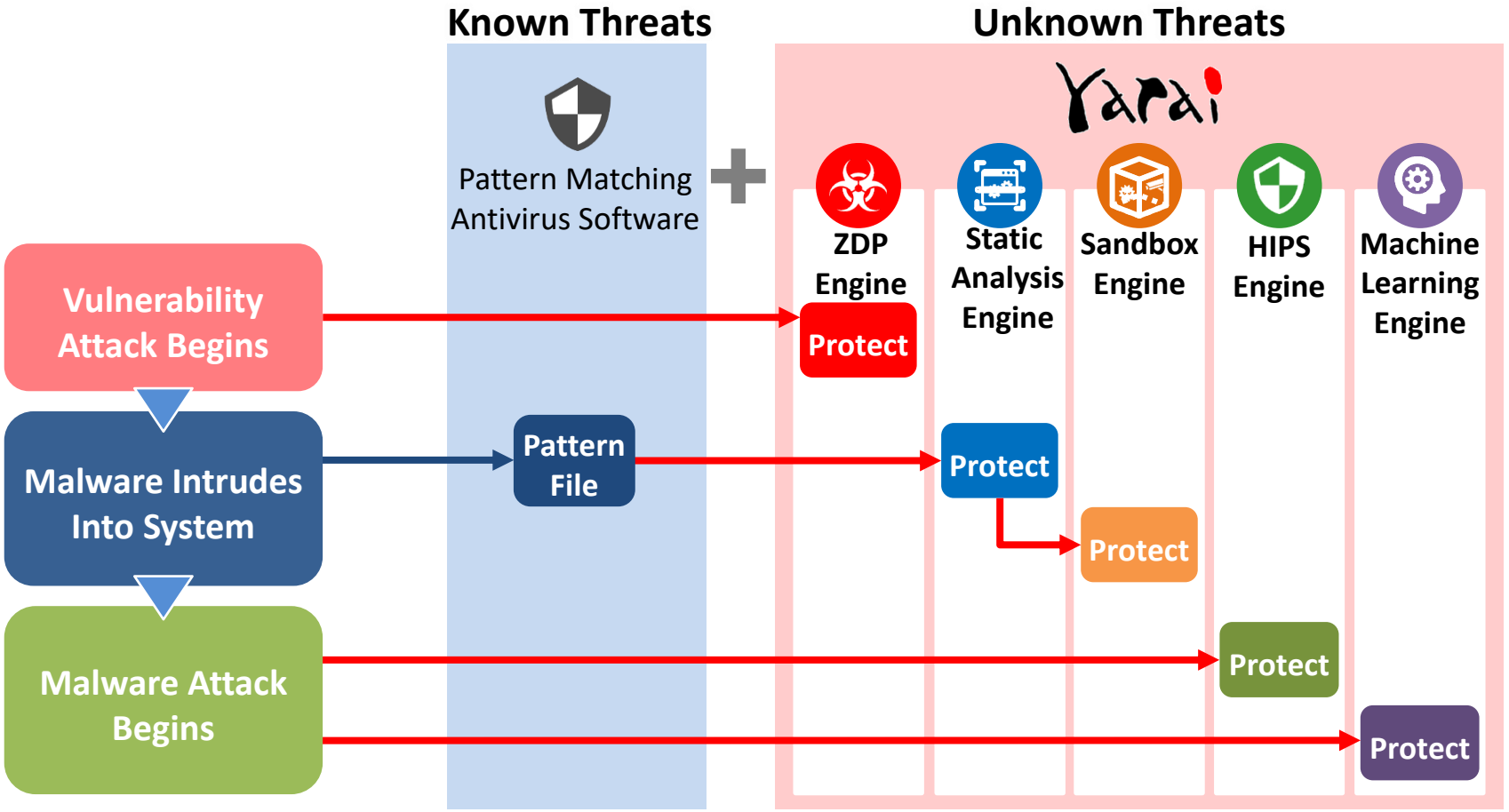


- Verification Environment
  Windows 7 x FFRI yarai 2.9.0 (Released in May 2017)
- Hash value of sample verified (SHA-256)
  2781526f6b302da00661b9a6a625a5a6ecf4ffccafa61202e9b0e9b61b657867

Endpoint “Multi-Layer Protection”

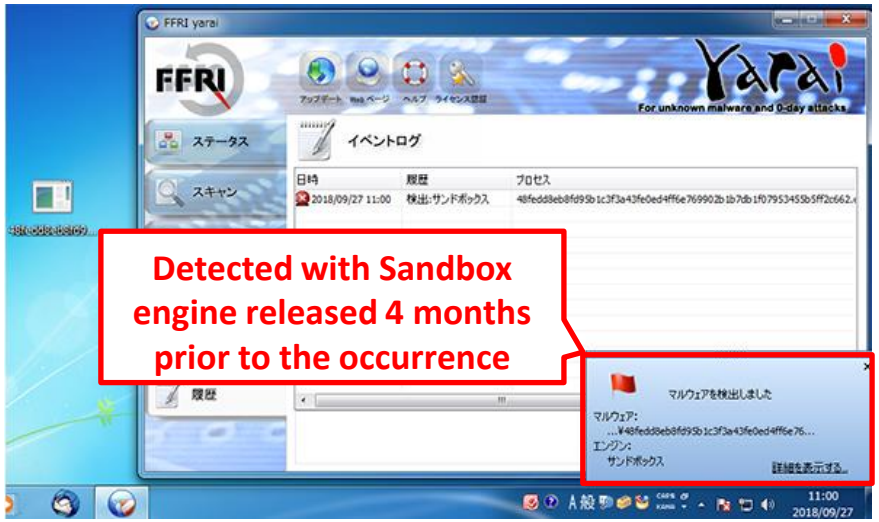
Windows 10 includes “Windows Defender” by default

Make your protection more robust by adding unknown threat protection



FFRI yarai vs ”Emotet” Malware

Occurrence / Reported Date	In July 2018, "Emotet", malware that self-propagates like a warm, is in prevalent affecting government institutions and companies, and a warning has been issued around the world.
Overview	"Emotet" malware was first reported as banking malware in 2014, however, it has been modified since to play the role of a loader to download other malware.
Attack Details	"Emotet" first uses a macro in a Word document. Microsoft Office disables macros by default, however, the malware infection starts when a user disregards the security warning and enables macros.



FFRI yarai blocking “Emotet” Malware

■ Verification Environment
Windows 7 × **FFRI yarai 2.11.4 (Released in March 2018)**

■ Hash value of sample verified (SHA-256)
48fedd8eb8fd95b1c3f3a43fe0ed4ff6e769902b1b7db1f07953455b5ff2c662

Track Record of FFRI yarai Protection (Unknown Malware)

Eliminating Malware Threats In Versions Released Before Exploitation In The Wild

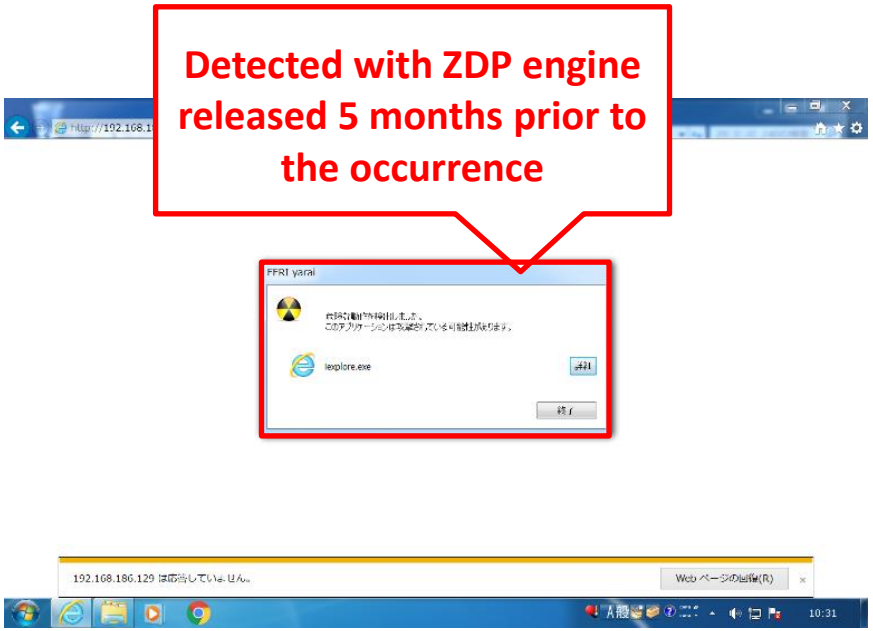
Occurrence/ Report Date	Protection Engine Release Date	Unknown Threat (at the time) and Targeted Attack	FFRI yarai Detection & Protection Engine
July 2019	January 2019	“Sodin” ransomware	HIPS Engine
April 2019	May 2017	Malicious Excel File Impersonating Invoice or Delivery Slip	HIPS Engine
January 2019	March 2018	"Anatova" Ransomware	HIPS Engine
August 2018	March 2018	Malware using Windows task scheduler	Static Analysis Engine
July 2018	March 2018	“Emotet” malware	Sandbox Engine
April 2018	June 2017	“Satan” ransomware	Static Analysis Engine
April 2018	June 2017	“GandCrab” ransomware	HIPS Engine
March 2018	June 2017	“Panda Banker” banking malware	HIPS Engine
January 2018	May 2017	“SpriteCoin” ransomware	HIPS Engine
January 2018	May 2017	“Rapid” ransomware	Static Analysis Engine
December 2017	May 2017	“CoinMiner” cryptocurrency mining malware	HIPS Engine
December 2017	May 2017	Malware impersonating “Rakuten Card Co., Ltd”	HIPS Engine
October 2017	January 2017	“Bad Rabbit” ransomware	Static Analysis Engine
May 2017	October 2016	“WannaCry/WannaCrypt”ransomware	Static Analysis Engine
January 2017	September 2016	“Mirai”IoTmalware	Static Analysis Engine
June 2015	August 2014	"Emdivi" malware targeting the Japan Pension Service	(Not published)

※The release dates for protection engines are approximately 1 month to 1 year before the unknown threats or targeted attacks occurred. This means that "proactive technology" was used to detect and protect against future threats with a protection engine developed before such threats were even known.

※This protection record was obtained internally based on the results of verification against samples and does not guarantee the detection of all variants.

FFRI yarai vs VBScript Vulnerability (CVE-2018-8174)

Occurrence / Reported Date	On May 9th, 2018, Microsoft released a security update for Windows VBScript Engine Remote Code Execution Vulnerability "CVE-2018-8174". Microsoft announced the confirmed exploitation in the wild and urged users to apply the hotfix immediately.
Overview	This vulnerability allows the remote code execution when VBScript engine handles objects in memory.
Attack Details	In case this vulnerability is exploited, an attacker could cause various damages such as: ・unexpected termination of application programs ・an attacker takes control of an affected system



FFRI yarai blocking the vulnerability attack using CVE-2018-8174

■ Verification Environment
Windows 7 × **FFRI yarai 2.11.0 (Released in December 2017)**

Track Record of FFRI yarai Protection (0-day Attacks)

Eliminating Vulnerability Attacks In Versions Released Before Exploitation In The Wild

Occurrence /Report Date	Protection Engine Release Date	Unknown Threat (at the time) and Targeted Attack	FFRI yarai Detection & Protection Engine
December 2018	March 2018	Adobe Flash Player 0-Day Vulnerability (CVE-2018-15982)	ZDP Engine
May 2018	December 2017	VBScript Vulnerability (CVE-2018-8174)	ZDP Engine
May 2018	December 2017	Adobe Acrobat, Adobe Reader Vulnerability (CVE-2018-4990)	ZDP Engine
January 2018	June 2017	Adobe Flash Player Vulnerability (CVE-2018-4878)	ZDP Engine
January 2017	July 2015	Firefox Vulnerability (CVE-2017-5375)	ZDP Engine
July 2015	November 2013	Adobe Flash Player Vulnerability (CVE-2015-5119, CVE-2015-5122)	ZDP Engine
June 2015	November 2013	Adobe Flash Player Vulnerability (CVE-2015-3113)	ZDP Engine
January 2015	December 2014	Adobe Flash Player Vulnerability (CVE-2015-0311)	ZDP Engine
November 2014	August 2014	Ichitaro 0-day Vulnerability (CVE-2014-7247)	ZDP Engine
February 2014	November 2013	IE 0-day Vulnerability (CVE-2014-0322)	ZDP Engine

* The release dates for protection engines are approximately 2 months to 20 months before the unknown threats or targeted attacks occurred. This means that "proactive technology" was used to detect and protect against future threats with a protection engine developed before such threats were even known.

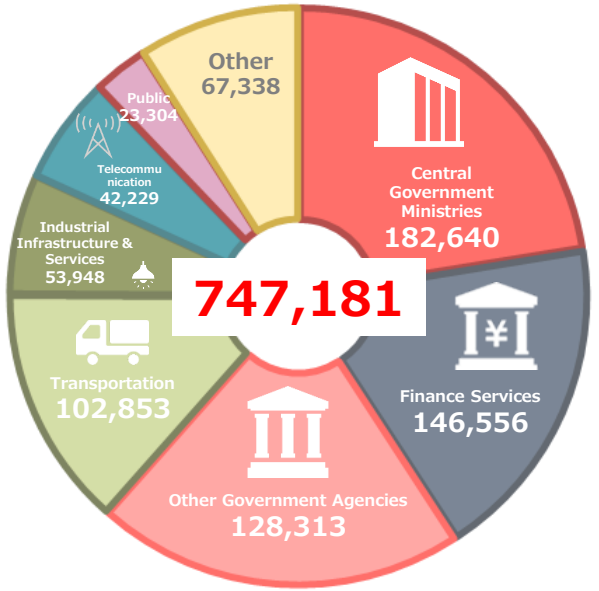
FFRI yarai License Track Record

Case Studies

- Sony Bank Incorporated
- Tokushima Prefectural Government
- Kanagawa Chuo Kotsu Co., Ltd.
- Hanshin Expressway Company Limited
- Hanshin Expressway R&D Company Limited
- Fujikura Ltd.
- SMBC Nikko Securities(Hong Kong) Limited
- DENSO Products and Services North America, Inc.
- Aoyama Gakuin University

Academic licenses and OEM product achievements are also available on the FFRI Security website.
https://www.ffri.jp/products/yarai/example.htm

Number of Contract Licenses by business



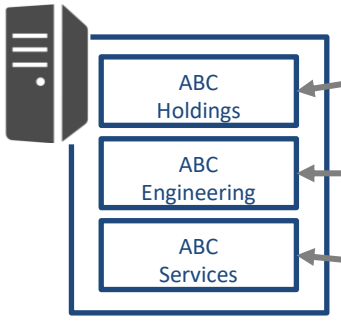
Source: <https://ssl4.eir-parts.net/doc/3692/ir_material14/121473/00.pdf>

Trusted to Protect Government & Critical Infrastructure

Management Console “FFRI AMC”

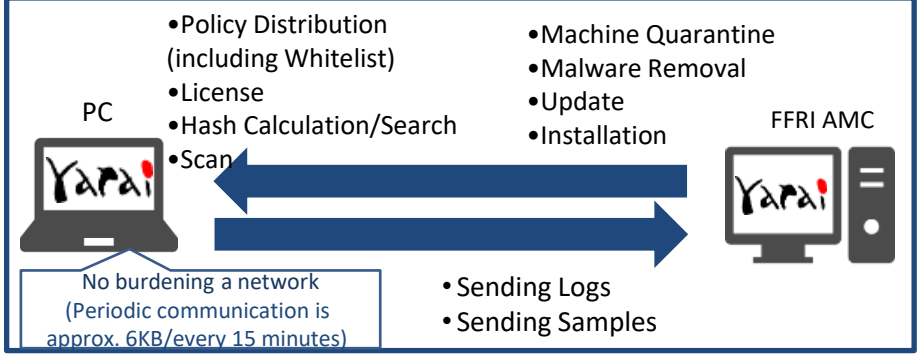
"FFRI AMC “ (free of charge) allows to centrally manage clients, log collection, incidents, malware sample collection and policy distribution

Support Multi-Tenant Environment



- Multiple organizations can be managed by a single server
- No need to purchase and configure a server for each organization - saving server cost

Communication/Management



Effective Data Breach Protection & Security Monitoring/Operation for Whole Organization

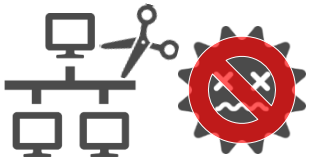
EDR (Endpoint Detection and Response) Feature

Bundles EDR features required for operation (no additional charge)
Specializing on simple features such as "Threat Search", "Removal" and “Isolation"
Allows operation without a security specialist

Hunting Feature

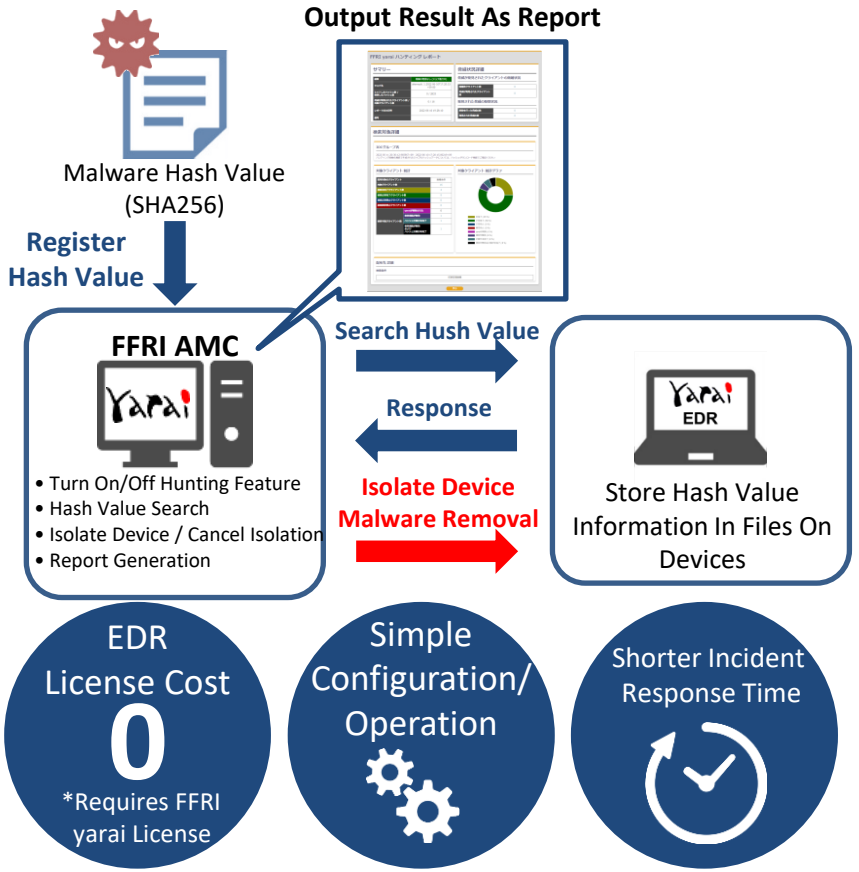
Investigate if threat exists within an organization by entering threat information (malware hash value) into FFRI AMC and matching it with hash values in files on devices

Response Feature



For malware found by the hunting feature:

- Malware Removal
- Isolate device confirmed with malware infection



Operating Environment

	FFRI yarai		FFRI AMC
OS	Windows 7 Windows 8.1 Windows 10	Windows Server 2012/2012 R2 Windows Server 2016 Windows Server 2019	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Hardware Environment	■ CPU 1 GHz or higher (Dual Core Required) ■ Memory 2 GB or higher ■ Hard Disk More than 1 GB free space ■ File System System and installation drives require NTFS ■ Virtual Environment Supported		■ CPU 4 cores or more ■ Memory 8 GB or higher ■ Hard Disk At least 100 GB of free space ■ NIC GbE * Terms of Use • This is the minimum requirements for a management console server to operate. The maximum number of clients that AMC is able to handle depends on the network configuration and server environments. • Above requirements are approximately for 30,000 clients, and it might require more than the above depending on the number of clients to manage.

*Refer to FFRI Security website for further details regarding the operating environments for FFRI yarai and FFRI AMC: https://www.ffri.jp/products/yarai/requirement.htm

Antivirus Software that can co-exist with FFRI yarai (vendor names)
Microsoft, Symantec, McAfee, F-Secure, Sophos, TrendMicro, ESET,

*Refer to FFRI Security website for details such as product names and version information: https://www.ffri.jp/products/yarai/requirement.htm

*TrendMicro and ESET can coexist only on Japanese OS.

Thanks.

2022.11.08
ASEAN-Cyber Business Platform Project Networking Session @Bangkok

Taked by Norihiko MAEDA (norihiko.maeda@ffri.jp)
Director of CEO Office
FFRI Security, Inc.

https://www.ffri.jp/en/index.htm