Company Profile

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

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 :   ¥265,231,300 (as of November 30, 2015)

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
* This vulnerability was discovered with our **FFR Raven** inspection tool.

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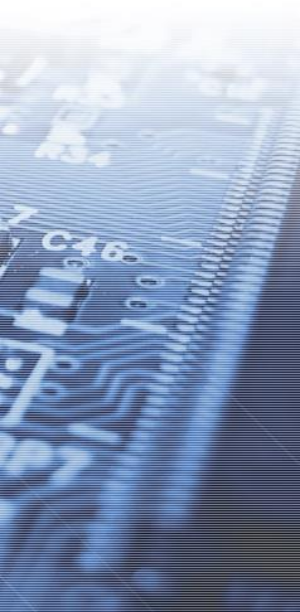
"Windows Phone 7 Internals and Exploitability" (Black Hat USA 2012)
http://www.ffri.jp/assets/files/research/research_papers/wp7-internals-and-exploitability.pdf

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**

Protection against targeted attack malware, known malware, known and unknown security vulnerability attacks, without reliance on patterns.
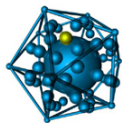
✅ **Targeted Attack Malware Inspection Service**

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**

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

✅ **Security inspection before shipment for embedded devices**

Raven レイブン Product Security Testing Suite

Inspects security robustness of network capable embedded devices. Discovers unknown security vulnerabilities by fuzzing.

- Personal & SOHO -

✅ **Next Generaion Endpint Security**

yarai Home and Business Edition

Stand-alone version of "FFRI yarai" Next-generation endpoint security product for personal and SOHO environment, which provides protection against unknown threat by our unique proactive defense technology.

✅ **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 for IoT Devices

IoT Devices·System Security Inspection Service

Threat analysis and inspections for pre-shipping IoT devices and systems by our research team who has enough experiences and output at international conferences.

✅ 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.

Outsourced Development and Other Services (FY2014 Track Record)

Business	Category	Details
Government Agency	Education/Training	Malware analysis training using analysis tools
	Education/Training	Security training for emergency security response personnel
	Education/Training	Malware network analysis training
	Research	Research regarding the capture and analysis of cyber attack information
		Study of latest malware trends
		Study of the effects of cyber attacks
		Research regarding the analysis and detection of cyber attacks
		Research regarding protection against cyber attacks
	Analysis	Detailed malware analysis service
Telecommunications	Education/Training	CSIRT/SOC personnel training support
	Research	Study of security regarding USB devices
		Study of trends in cyber security
	Outsourced Development	Development of modules for endpoint security
		Development of monitoring modules for information leakage protection software
	Investigation/Diagnosis	Investigation of router security
		Investigation of security appliance security
		Investigation of UTM security
		Investigation of router security
		Diagnosis of network device vulnerability
Electronics	Education/Training	Security training for information system administrators
	Research	Investigation of security technology for control systems
	Investigation/Diagnosis	Investigation of vulnerabilities in Android smartphones
Financial Services	Investigation/Diagnosis	Diagnosis of Web API security
		Detailed analysis of MITB malware
Industrial Infrastructure/Services	Education/Training	Security technician training, dynamic malware analysis, reverse engineering, vulnerability analysis
	Investigation/Diagnosis	Diagnosis of Android tablet security

Security Solutions for Malware and Vulnerability Attacks

DMZ

In-house LAN

Internet

Attacker

Malware Distribution Site

C&C Server

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.

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.