ERADICATE APT/RANSOMWARE !

New/Variant Malware Response Solution

Zombie ZERO

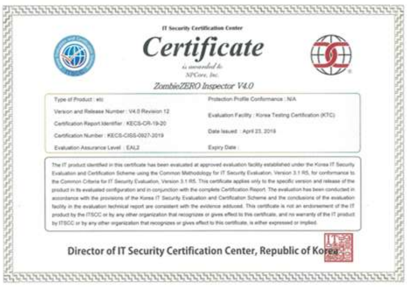
International CC & GS Certification: Grade 1

K-INNOVATIVE PRODUCT

GOOD Software

Detecting/blocking New/Variant Malware such as Ransomware and APT (Advanced Persistent Threat)

ZombieZERO SECaaS EDR



IT Security Certification Center

Certificate

is awarded to

NPCore, Inc.

ZombieZERO Inspector V4.0

Type of Product : etc	Protection Profile Conformance : N/A
Version and Release Number : V4.0 Revision 12	Evaluation Facility : Korea Testing Certification (KTC)
Certification Report Identifier : KECS-CR-19-20	Date Issued : April 23, 2019
Certification Number : KECS-CISS-0927-2019	
Evaluation Assurance Level : EAL2	Expiry Date :

The IT product identified in this certificate has been evaluated at approved evaluation facility established under the Korea IT Security Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 R5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 R5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Korea IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the ITSCC or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by ITSCC or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Director of IT Security Certification Center, Republic of Korea

New/Variant Malware Response Solution

ZombieZERO SECaaS EDR

Product Specific Feature - ZombieZERO SECaaS EDR

Detect/Block Ransomware Behavior

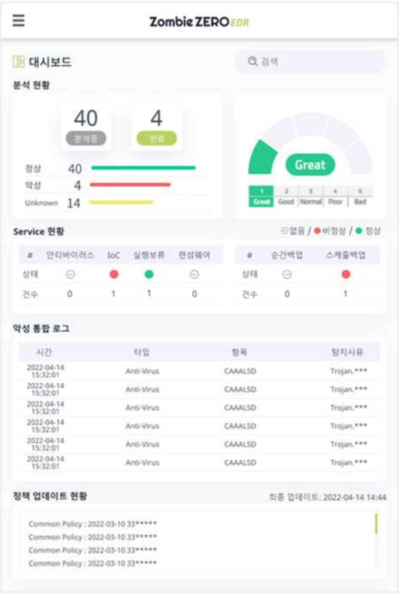
Detect and block real-time ransomware behavior
Response to the file encryption and forgery

ZeroTrust Security

When a new file is inflowed or a threat file
is executed, the file execution is pending,
and the file is uploaded to the analysis server

Bitdefender's AV Function

Support the Global vaccine Bitdefender AV function
Rapid proactive detection of malicious code



분석 현황

40 분석중

4 완료

정상	40
악성	4
Unknown	14

Service 현황

⊝ 없음 / ● 비정상 / ● 정상

#	안티바이러스	IoC	실행보류	랜섬웨어
상태	⊝	●	●	⊝
건수	0	1	1	0

#	순간백업	스케줄백업
상태	⊝	●
건수	0	1

악성 통합 로그

시간	타입	항목	탐지사유
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***
2022-04-14 15:32:01	Anti-Virus	CAAALSD	Trojan.***

정책 업데이트 현황

최종 업데이트: 2022-04-14 14:44

Common Policy : 2022-03-10 33*****
Common Policy : 2022-03-10 33*****
Common Policy : 2022-03-10 33*****
Common Policy : 2022-03-10 33*****

(User’s UI)

Software Specification

Detection of Malicious Code

Detection and Analysis of APT and New and Variant Malicious Code

·Based on IOC(Indicators of Compromise) analysis of malicious behavior on endpoint behavior
·Detect/block ransomware based on behavior in real time and respond to Data Forgery and Tampering
·Zero Trust Security allows programs to run unverified programs pending and only running verified
·Using the official ECSC linkage of the Cyber Safety Center of the Ministry of Education, malicious code is analyzed using YARA Rule pattern

VM Sandbox Operation

Virtual Machine Sandbox Dynamic Analysis System

· Virtual machine sandbox dynamic analysis system provides analysis capabilities in closed network environments
· Support for manual updates and manual analysis of suspicious files in an Internet-blocked environments
· Provide dynamic behavioral analysis similar to real machine configuration with virtual machine bypass prevention

Security

Proven Reliability and Endpoint Centric Protection

· It blocks the possibility of malicious code infection through the execution hold analysis function of the first executable
· Ability to back up files to secure folders that are not accessible by normal processes, just before they start tampering with files
· Run backups at the kernel driver end, minimizing application conflict issues and performance degradation
· Backing up files centered on extensions / restoring backup files through a separate UI

Convenience

Delivering Convenience through Technology- Intensive Design

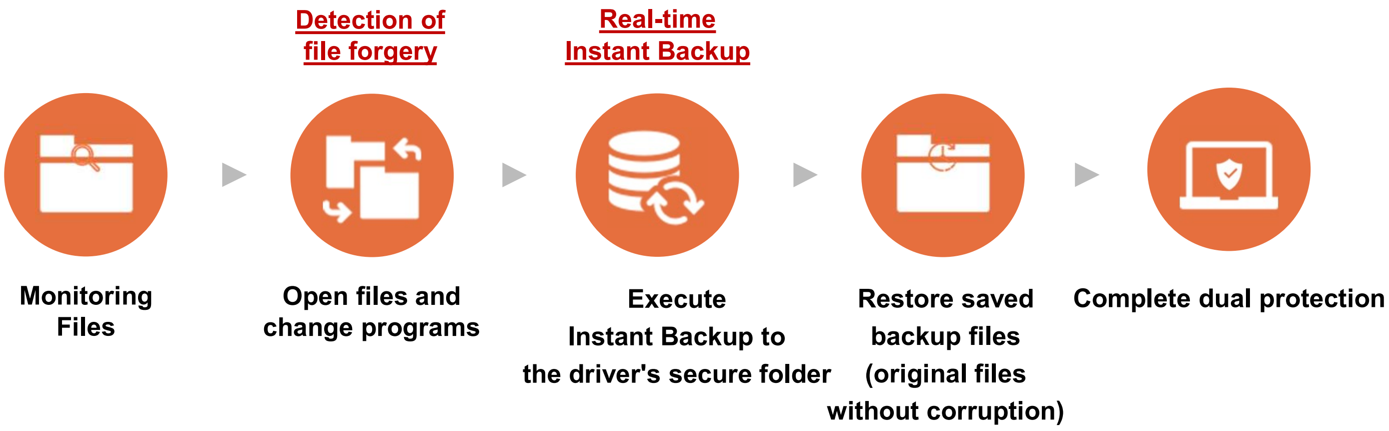
· Provides a function to apply differential security policies by organization/group
· Only Whitelist-Based Validated Processes Operate
· Blocking the Enable/Stop Real-Time Agent Monitoring feature
· Backing up files centered on extensions / restoring backup files through a separate UI
· Provides analysis reports and key alarms / provides integration with control solutions using Syslog

Utilize linked API

Securing Detection Rates through linking with API

· Quick detection/blocking of known malicious code via built-in AV engine (Bit-defender)
· Additional search function using Virus Total (requires purchase of a license separately)
· Reputation analysis integrating with global and domestic patterns

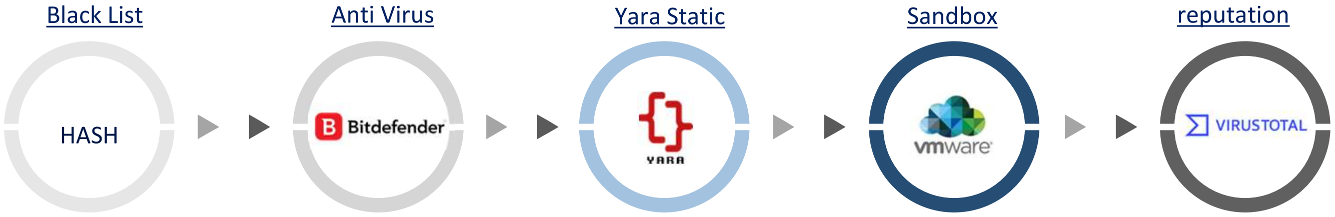
Real-time Instant Backup


Detection of file forgery
Real-time Instant Backup
Monitoring Files
Open files and change programs
Execute Instant Backup to the driver's secure folder
Restore saved backup files (original files without corruption)
Complete dual protection

EDR is a security solution that proactively detects and blocks malicious code,

Instant backup provides greater information security

Multi-dimensional Analysis



NPCORE

ISBiz Tower 1001, 26, Yangpyeong-ro 21-gil,
Yeongdeungpo-gu, Seoul, R.Korea

Tel 02-1544-5317 / **Fax** 02-413-5317 www.npcore.com

Tel **+82-02-1544-5317**

Tech Support **070-7834-8060**
Product Inquiry / Request For Quotation
sales@npcore.com

CERTIFICATIONS

Grade 1

Weekdays: 10:00 am - 7:00 pm (excluding Saturdays, Sundays, and public holidays)