RevBits®

PRODUCT BRIEF

Phoenix

RevBits Detection and Response Engine Blocks Cyberbreaches Before They Begin.

Phoenix is RevBits' powerful, feature-rich exploit detection and response engine within our endpoint solutions, including EDR, XDR and Email Security products. The Phoenix engine effectively blocks breaches by detecting and blocking known and unknown (0-day) exploits. Exploit-based cyber threats are eliminated, before their shellcode or payload can be executed, spreading malware and stealing credentials.

Differentiating exploits from threats like malware and phishing

Understanding how exploits work, and their relationship to malware, is important. An exploit is the medium that is used to enable malware to enter into a computer system, application, file or web page. An exploit is the method of abusing a vulnerability that will lead to code execution. The code usually executed within exploits will lead to dropping a malware, backdoor or stealing sensitive files, which all can be done with the embedded shellcode in exploit. Shellcode is written in assembly and uses a sequence of commands that can take advantage of a computer and install malware. Such behavior includes gaining control of a computer system to obtain privileged escalation and disseminate malware.

RevBits Endpoint Security (EPS) includes EDR capabilities for centralized visibility and endpoint control.

Phoenix detects and eliminates exploits that might be coming through a phishing attack, drive-by downloads, malicious attachments with 0-days, and malicious webpages that are used to inject malware.

Cyber attackers will always go after the most widely consumed software or applications. The most popular, and therefore, the most commonly exploited software are Microsoft Office applications, like Word, Excel, PowerPoint and others; popular web browsers like Chrome, Firefox, Safari, Chromium, Internet Explorer, Edge, and others; and Adobe Flash Player (though retired now) and Acrobat Reader.

Phoenix protects all of these applications, and any other application that system admins choose to be protected. Without any specialized knowledge, administrators can effectively begin protecting their applications immediately after installation.

The hacker who created the exploits can execute a custom shellcode directly from the vulnerable application. Shellcode is a small piece of code, consisting of a long list of assembly / machine instructions that is executed after exploiting a software vulnerability. Bad actors like to use exploits because they don't require users to tap, click or swipe anything. The exploit code will be inserted into a format that a vulnerable application will parse and read, such as a PDF file, a webpage or an Office document file. Once the innocent looking file is opened or a webpage is visited, a specially crafted exploit will trigger the vulnerable code, exploit the vulnerability, and subsequently execute the shellcode that can lead to full compromise of the system. When this occurs, it will be a challenging job for analysts to find a link between the dropped malware or executed shellcode, and original source of the exploit.

Rather than detecting a specific malware payload, Phoenix will block the exploit before an attack chain can begin, creating a definitive defense against an always changing threat surface.

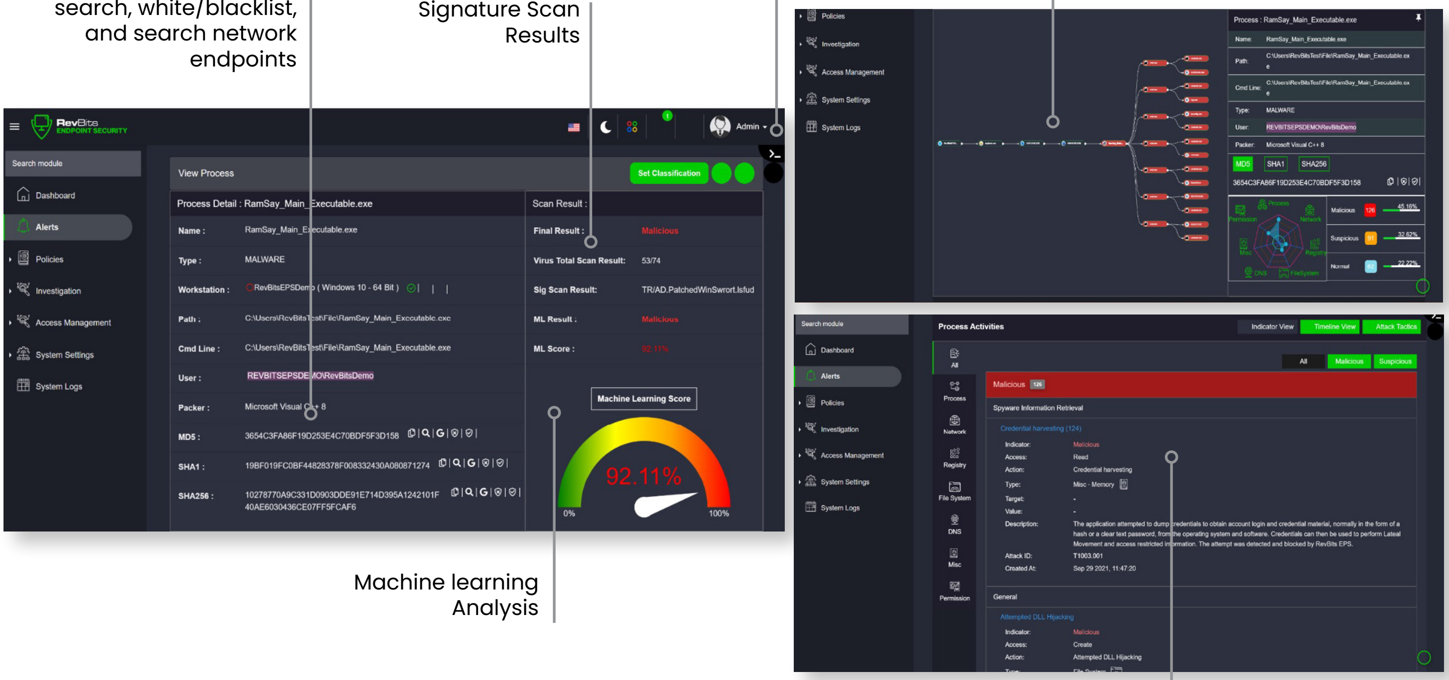
PowerShell - a two-edged sword

Admins use PowerShell to find security holes in their IT systems, automate tasks and manage configurations. Hackers also take advantage of PowerShell, by running file-less malware through it, making it difficult for anti-virus solutions to detect. Hackers use PowerShell as a remote-control tool, capturing and retrieving user credentials, without leaving any evidence or trail. If a hacker steals credentials by exploiting a Microsoft Office application or any browser or PDF file, the protections of a privileged account management (PAM) solution can be undermined. This is just another reason why a multi-layered security platform is so important.

When a hacker identifies a vulnerability within an application, like Microsoft Word, they will craft a special structure, packet or field to overflow a buffer, or create a heap overflow, leading vulnerable software to execute unintended code. They may overwrite the function return address with carefully crafted Return Oriented Programming (ROP) gadgets that can lead to arbitrary shellcode or machine code commands that Word is not supposed to run. This is an action that should never occur, and will allow hackers to run any command on the system, including code to download and execute remote malware, open a backdoor shell access for attackers to steal credentials, and so on.

Reliable, stable and scalable exploit and malware protection

A key attribute of Phoenix is that it has been comprehensively tested, and will not violate the stability of computer systems or applications. It is fully compatible with all Office applications, popular



Process Detail : RamSay_Main_Executable.exe

Name : RamSay_Main_Executable.exe
Type : MALWARE
Workstation : RevBitsEPSDemo (Windows 10 - 64 Bit)
Path : C:\Users\RevBitsTest\File\RamSay_Main_Executable.exe
Cmd Line : C:\Users\RevBitsTest\File\RamSay_Main_Executable.exe
User : REVBITSEPSDEMO\RevBitsDemo
Packer : Microsoft Visual C++ 8
MD5 : 3654C3FA86F19D253E4C70BDF5F3D158
SHA1 : 19BF019FC0BF44828378F008332430A080871274
SHA256 : 10278770A9C331D0903DDE91E714D395A1242101F 40AE6030436CE07FF5FCAF6

Scan Result :

Final Result : Malicious
Virus Total Scan Result: 53/74
Sig Scan Result: TR/AD.PatchedWinSwrort.lsfud
ML Result : Malicious
ML Score : 92.11%

Process : RamSay_Main_Executable.exe

Name: RamSay_Main_Executable.exe
Path: C:\Users\RevBitsTest\File\RamSay_Main_Executable.exe
Cmd Line: C:\Users\RevBitsTest\File\RamSay_Main_Executable.exe
Type: MALWARE
User: REVBITSEPSDEMO\RevBitsDemo
Packer: Microsoft Visual C++ 8
3654C3FA86F19D253E4C70BDF5F3D158

Malicious 126 45.16%
Suspicious 91 32.62%
Normal 62 22.22%

Malicious 126

Spyware Information Retrieval

Credential harvesting (124)

Indicator: Malicious
Access: Read
Action: Credential harvesting
Type: Misc - Memory
Target: -
Value: -
Description: The application attempted to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateal Movement and access restricted information. The attempt was detected and blocked by RevBits EPS.
Attack ID: T1003.001
Created At: Sep 29 2021, 11:47:20

General

Attempted DLL Hijacking

Indicator: Malicious
Access: Create
Action: Attempted DLL Hijacking

Multi-hash with single click to Google search, white/blacklist, and search network endpoints

Signature Scan Results

Single click to command line functionality

Execution process tree

Malicious executed command line

Machine learning Analysis

Behavioral analysis diagnosis

RevBits Endpoint Security's (RB-EPS) main alert dashboard for an individual workstation. RB-EPS provides a feature rich robust GUI.

browsers and Adobe files. Phoenix is highly scalable, and will report every attack and every potential threat through the RevBits Endpoint Security Console and/or Cyber Intelligence Platform (CIP) dashboard. This provides complete information about the infected web page, application or file, to localize the attack source and prevent further potentially unsafe actions. The technology works by monitoring endpoints, and collecting data into a centralized repository, where the data is analyzed and can be quickly acted upon.

Phoenix protects against Remote Code Execution (RCE) attacks. It also protects against Local Privilege Escalation (LPE) threats, where a web browser, system or application has a vulnerability that can be exploited to elevate access to a privileged account. Phoenix monitors and blocks exploitation methods, using various technologies, such as buffer overflow detection, HeapSpray protection, Export Address Filtering, Address Space Layout Randomization, Return Oriented Programming migrations, and many others.

> **“Most anti-virus and nextgen solutions can’t prevent exploits. Instead, they allow exploits to enter, and rely upon their ability to detect and mitigate the injected malware. This is like allowing a burglar to enter your house, and then trying to extricate them before they cause harm.”**

RevBits combines exploit and malware detection and response capabilities

RevBits is unique, in that is has both exploit and malware detection and response capabilities. Phoenix is essentially a DLL that injects into processes that are commonly and constantly exploited in widely used applications, web browsers, and PDF files. Phoenix can also protect legacy and custom applications. Any exploitation attempts will be thwarted, and no shellcode will ever be allowed to execute. Phoenix detects, blocks and kills any type of shellcode execution process, like buffer, heap, and integer overflows, before a shellcode is run and allowed to drop its malware.

Phoenix has no hooks into the applications themselves, but monitors and analyzes memory allocations, code calls and function structures, and installs hooks into the APIs associated with the applications. This makes it extremely stable and reliable. It will detect all exploits without creating false positives, and will not crash the applications. It has been thoroughly tested on Microsoft Windows and all Office applications, all popular web browsers, and on Adobe Flash Player, Acrobat Reader and PDF files. Phoenix has also had extensive exploit testing for Common Vulnerabilities and Exposures, or CVEs.

Security solutions must eliminate exploit entry

Most anti-virus and nextgen endpoint security solutions can’t prevent exploits. Instead, they allow the exploit to enter, and rely upon their ability to detect and mitigate the injected malware. This is like allowing a burglar into your house, and then trying to extricate them before they cause harm. As evidenced by the number of breaches occurring on a daily basis, cyberattacks are increasingly more difficult to discover, and cyber threats should not be tolerated at any point in the attack chain. They must be eliminated at point zero (at the exploit), before they are allowed to drop their malware.

Keep Your Enterprise Protected. Get a Demo or Free Evaluation.
To learn more, visit www.revbits.com