ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 01/23/2020 by Deyka Atencio

Increased Emotet Malware Activity

01/22/2020 23:15

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of a recent increase in targeted Emotet malware attacks. Emotet is a sophisticated Trojan that commonly functions as a downloader or dropper of other malware. Emotet primarily spreads via malicious email attachments and attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. If successful, an attacker could use an Emotet infection to obtain sensitive information. Such an attack could result in proprietary information and financial loss as well as disruption to operations and harm to reputation.

CISA recommends users and administrator adhere to the following best practices to defend against Emotet. See CISA's Alert on Emotet Malware for detailed guidance.

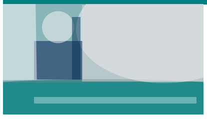
- Block email attachments commonly associated with malware (e.g.,.dll and .exe).
- Block email attachments that cannot be scanned by antivirus software (e.g., .zip files).
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the email gateway, and block suspicious IP addresses at the firewall.
- Adhere to the principle of least privilege.
- Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system.
- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.

CISA encourages users and administrators to review the following resources for information about defending against Emotet and other malware.

- CISA Alert Emotet Malware
- Australian Cyber Security Centre (ACSC) Advisory Emotet Malware Campaign
- CISA Tip Protecting Against Malicious Code

10 Best Advanced Endpoint Security Tools of 2020

01/23/2020 05:31



Every enterprise, regardless of size, has what we call a digital perimeter. This perimeter is comprised of all the devices, or endpoints, which connect to your IT network and their cybersecurity protections. In this article, we list the 10 Best Advanced **Endpoint Security Tools**.

These can include laptop and desktop computers, as well as mobile and IoT devices. As more individuals connect to your network, the larger and more porous your digital perimeter becomes, making potential infiltrations by hackers.

Why Endpoint Security Important

You can think of each connecting endpoint as a new gateway for both users and hackers to access your most important digital assets. And not only that, even the endpoints themselves can become the target of various cyber-attacks, including ransomware, cryptojacking, phishing, and fileless malware.

Generally, not every endpoint connecting to your business IT infrastructure provides a consistent layer of cybersecurity; some only use their default protections, which prove woefully inadequate against hackers. This is where endpoint security steps in.

Next-generation Endpoint Security

Next-generation **endpoint protection** allows IT, security teams to monitor and secure all connected devices from a centralized location, ensuring consistent protection across the network.

With next-generation antivirus capabilities, endpoint protection prevents, detects, and removes cyber threats like ransomware that would otherwise penetrate your initial defenses. However, **Endpoint Security** does so much more than that. Here we have an example, sandboxing IT members can analyze and evaluate unknown programs by safely observing their behaviors.

Through EDR, **endpoint security tools** can uncover dwelling threats and alert your security team. Next-generation firewalls monitor digital traffic coming into and leaving the network, tracking and blocking malicious or suspicious traffic and domains.

And with application control, you can extend your cybersecurity to the data collected and transferred through apps on your devices. Hence, endpoint protection is a necessary building block for any enterprise nowadays. Here you can find the Endpoint protection reviews.

What is EPP (Endpoint Protection Platforms), and why it's essential?

EPP (Endpoint Protection Platforms) are traditional security solutions that have been around the enterprise for a little over thirty years. They generally provide anti-malware protection and have an element of the machine learning in them.

Generally, Antivirus programs cover all the options for regulatory, governance, and compliance audits, but they offer organizations limited benefits in terms of security. Although antivirus solutions protect virtually all endpoints and servers in the world, however, the security breaches continue to occur at an alarming rate.

This is mainly because traditional antivirus is a signature-based security tool that focuses on detecting known threats and responding to them once they have penetrated the network. Expert attackers can circumvent the antivirus with automated and cheap online tools that generate countless unique and unknown attacks.

Hence, **endpoint solutions** are being required by security teams to be that primary tool an incident occurs to help identify the scope and impact of how this malware got into the environment and where it may have gone now.

In short, **Endpoint Security Tools** simply protects your enterprise or home office network from things like malware, ransomware, and other major security threats.

Best Endpoint Security Tools of 2019

- **ESET Endpoint Security**
- **Trend Micro Apex One**
- **Symantec Endpoint Detection and Response**
- **Comodo Advanced Endpoint Protection**
- **CrowdStrike Falcon Insight**
- **Cybereason Total Enterprise Protection**
- **Malwarebytes Endpoint Protection**
- **Panda Endpoint Protection**
- **FireEye Endpoint Security**
- **Stormshield Endpoint Security**

ESET Endpoint Security

ESET is generally created for mobile networks and workforces, with simple deployment and lightweight solutions. It will be of benefit to SMBs without a dedicated IT department asking a simplified and effective anti-malware software that will not endanger their business speed. Hence, they were named in the Gartner Magic Quadrant research.

ESET Endpoint Security Image Credits: ESET

Business **endpoint security tools** provide proactive protection against all types of online and offline warnings and prevent malware from reaching other users. Antivirus and Antispyware are produced for working environments with a variety of features for seamless service and high production.

An individual layer of protection isn't enough in today's regularly growing threat aspect. Hence, all ESET endpoint products can identify malware pre-execution, while execution and post-execution. And by concentrating on the whole malware lifecycle, ESET grants the highest level of protection possible.

Key features of ESET Endpoint Security:-

- Indicator of attack
- Behavioral detection
- Network attack protection
- Two-Way firewall
- In-Product sandbox
- Malware protection
- SPAM protection
- Web filtering

Trend Micro Apex One

Concentrating on multi-layered protection, exploitation security, and machine learning, Trend Micro allows a full set of EDR and EPP solutions, so that it should fit with the demands of every buyer.

Trend Micro Apex One*Image Credits:* Trend Micro

For SMBs and big companies, Trend Micro is one of the best choices, as it offers **endpoint protection**, data protection, and cloud security. Trend Micro serves to ensure mobile and desktop protection, and it proceeds to research enterprise security as well.

The best part of this product is that its utility to set up the whole Trend Micro ecosystem to the endpoints with a vast rate of detection and a very granular detection information system.

Key features of Trend Micro Apex One:-

- Pre-Execution and runtime machine learning
- Advanced Malware prevention system
- Effective protection
- Detects vulnerability
- Indicator of attack
- Indicator of compromise (IOCs)

Symantec Endpoint Detection and Response

Symantec Endpoint Detection and Response (EDR) Cloud gives in-depth endpoint clarity, automatic threat hunting, and breach defense over the whole undertaking. Symantec EDR is a cloud-based service that can be used in minutes and helps to establish a firm's security position against cyber attacks.

Symantec Endpoint Detection and Response *Image Credits: Symantec*

In short, we can say that Symantec **Endpoint detection and response** (EDR) is a kind of tools and technology used for preserving computer hardware devices, known as endpoints, from possible threats.

EDR programs are made from tools that concentrate on identifying possible malicious endpoint movements, generally through employing continuous monitoring. Ideally, EDR gives an organization with endpoint prominence through collecting data from endpoint devices and then uses that data to detect and react to potential outside threats.

Key features of Symantec Endpoint Detection and Response:-

- Unification of endpoint data
- Increased visibility through IT environment
- Ability to monitor endpoints
- Ability to detect malware
- Integration tools
- Proper use of blacklist and whitelist

Comodo Advanced Endpoint Protection

The Comodo organization is a worldwide innovator and developer of cybersecurity solutions. The new Comodo Advanced **Endpoint Protection** solution simply defends organizations against both known and unknown malware by working on all hidden files in automated containment.

Comodo Advanced Endpoint Protection *Image Credits: Comodo*

The Comodo Advanced Endpoint Protection solution is created upon a Default Deny Platform, which provides known useful data, prevents known corrupt files, and much more.

Comodo has joined its advanced endpoint security solution and enterprise-class design management, including Comodo Advanced Endpoint Protection and Comodo Device Manager, and the File Analysis Platform Valkyrie into Comodo Advanced Endpoint Protection.

Key features of Comodo Advanced Endpoint Protection:-

- Integrated device management
- Application management
- Device security
- Anti-theft feature
- Automated containerization

CrowdStrike Falcon Insight

CrowdStrike allows visibility in real-time and identifies attacks inside your software, which includes Windows desktop and servers on Mac computers also, whether on or off and connects EDR and anti-malware into a single agent; hence, it’s an excellent appealing option for the enterprises of all sizes.

CrowdStrike Falcon Insight Image Credits: Crowdstrike

Moreover, CrowdStrike also offers a high degree of customization in its safety options and parameters and a managed threat hunting service for those users who is concerned about ongoing issues and unable to divert IT resources.

Key features of CrowdStrike Falcon Insight:-

- Remote visibility
- Indicator of attack
- Real-time visibility
- Five-second search
- Behavioral protection
- Insight and intelligence
- Immediate response
- Zero impact on endpoint

Cybereason Total Enterprise Protection

Cybereason automatically identifies malicious activity and performs it intuitively. Most of the organizations who use Cybereason, simply start identifying attacks within 24 to 48 hours. Cybereason Services assists customers in completing protection, identifying, receiving, and respond to security events.

Cybereason Total Enterprise Protection Image Credits: Cybereason

As its global team can increase your coverage, improve your processes and capabilities, and uplift your company’s protection posture with 24/7 monitoring, dedicated support, proactive threat hunting, and fast response to events, whether remote or onsite.

Basically, it provides complete **endpoint security**; hence, Cybereason EDR is a full-featured EDR solution that is created to identify, investigate, and remediate highly advanced warnings. Cybereason's in-memory graph reserves all event data and answers questions in seconds over tens of millions of events.

Key features of Cybereason Total Enterprise Protection:-

- Actionable threat detection
- Custom detection rule
- Remediation option
- Active hunting
- Active monitoring
- Active response
- Incident response
- Active assist

Malwarebytes Endpoint Protection

Malwarebytes **Endpoint Protection** is an excellent threat prevention solution for endpoints that uses a layered way with multiple exposure techniques. This gives businesses with full attack chain security against both known and unknown malware, ransomware, and zero-hour threats.

Malwarebytes Endpoint Security Image Credits: Malwarebytes

Malwarebytes Endpoint Security is one of the **endpoint security tools** that take all of our industry-leading endpoint security and remediation technologies into one cybersecurity solution.

This multi-layer protection model reveals the attack chain by combining advanced malware detection and remediation, malicious website blocking, ransomware blocking, and exploit security into a single solution.

Key features of Malwarebytes Endpoint Protection:-

- Multi-vector protection
- Integrated remediation capabilities
- Exploit mitigation
- Web protection
- Payload analysis
- Ransomware mitigation
- Application behavior
- Malwarebytes management console

Panda Endpoint Protection

Panda Security’s Adaptive Defense 360 includes traditional EPP and EDR clarifications as a single offering, giving continuous monitoring and blocking of endpoint-based activity. Hence, Panda offers EPP, email, web gateways, and PC management abilities; all addressed within a cloud-based management console.

Panda Endpoint Protection Image Credits: Panda

SMBs that are investigating easy-to-manage, cloud-based solutions should think Panda as a shortlisted listing in established geographies, and not only that, even they have also earned the Gartner Magic Quadrant.

It basically offers centralized and excellent protection for all of your Windows, Mac, and Linux workstations, including laptops and different servers, in addition to the first virtualization systems and Android Devices.

Key features of Panda Endpoint Protection:-

- Remedial action
- Monitoring and reports
- Profile-based protection
- Device control
- Alert monitoring
- Patch management
- Software deployment

FireEye Endpoint Security

FireEye include firewalls, IPS, antivirus, and gateways as a means of improving signature-based discovery methods. The FireEye platform uses a virtual execution engine with threat intelligence to detect and prevent cyber-attacks in real-time.

FireEye Endpoint Security Image Credits: FireEye

FireEye cybersecurity solution is basically designed with a wide range of skills to help security teams to identify, analyze, and defend against the advanced warnings targeting businesses today. Their solution is available to businesses of all sizes, offering simple solutions for small and medium-sized enterprises.

Key features of FireEye Endpoint Security:-

- End-to-end visibility
- Intelligence-led endpoint security
- Detection and response capabilities
- Respond at scale
- Light-weight multi-engine tool
- Enterprise security search

Stormshield Endpoint Security

A security situation usually depends on the perception of users and the responsiveness of signature-based tools, such as antivirus. Despite their investments in conventional security solutions, companies settle vulnerable.

Stormshield Endpoint Security Image: Stromshield

Stormshield Endpoint Security offers a corresponding layer of security to compensate for those weaknesses by assuring continuous power over behaviors on servers, workstations, and terminal devices according to fine-grained protection systems that put in place by the administrator.

Stormshield Endpoint Security controls optimal security requirements for environments that are subjected to strict limitations, like operational technology or point-of-sale devices. This real-time security is entirely natural and autonomous, and it does not influence workstations nor requires attachments to external systems.

Key features of Stormshield Endpoint Security:-

- Protects the global station
- Room for improvement
- Customer service and technical report
- Anti-exploit technology
- Endpoint detection and response
- Centralized management

Conclusion

According to us, these are some of the best **Endpoint Security Tools** in the open-source world, and the most interesting thing is that they all are user-friendly. So here, we have tried our best to provide all the information about the top 10 Advanced Endpoint protection Security Tools, so simply try them and see which one is better for you.

However, if you have any other **endpoint security tool** that you have used and think is most suitable and user-friendly, then please let us know in the comment section. We hope that you liked this post, and it must have been useful to you; if so, then do not forget to share this post with your friends, associates, and on your social profiles.

Also Read: Top 10 Best Open Source Firewall to Protect Your Enterprise Network 2019

Data on 30,000 Cannabis Users Exposed in Cloud Leak

01/23/2020 12:10

Tens of thousands of cannabis users in the US have had their personal information leaked by a misconfigured cloud bucket, according to researchers.

Over 85,000 files including more than 30,000 records with sensitive personally identifiable information (PII) were exposed when software firm THSuite apparently left an Web Services (AWS) S3 bucket unsecured.

THSuite provides software that helps cannabis dispensaries collect the large volumes of sensitive user info they need to comply with state laws.

At least three clients were affected in the privacy snafu: Amedicanna Dispensary, Bloom Medicinals and Colorado Grow Company.

Exposed PII included names, home and email addresses, dates of birth, phone numbers, medical ID numbers and much more, according to vpnMentor.

As such, the leak affected both medical cannabis users and those who bought the plant for recreational purposes.

"Medical patients have a legal right to keep their medical information private for good reason. Patients whose personal information was leaked may face negative consequences both personally and professionally," the researchers argued.

"Under HIPAA regulations, it's a federal crime in the US for any health services provider to expose protected health information (PHI) that could be used to identify an individual."

The revelations may also harm recreational users, especially if their employer prohibits cannabis use, they continued. The database apparently included scanned copies of government and employee IDs.

From a cybercrime perspective, the data trove would also offer a potentially lucrative opportunity for hackers to craft convincing phishing emails, texts and calls, and launch follow-on identity fraud attempts.

The researchers found the exposed database via a simple scan on December 24 last year. After contacting its owners on December 26 the problem was finally mitigated on January 14 2020.

Cloud misconfigurations like this remain a major source of cyber-related risk for organizations around the world. VpnMentor alone has been able to find millions of user records leaked by the likes of cosmetic giant Yves Rocher, Best Western Hotels and Canadian telco Freedom Mobile.

Singapore inks digital trade partnership with global group, firms

01/23/2020 12:35

Singapore has inked an agreement with the International Chamber of Commerce (ICC) and several global organisations to fuel the adoption of digital technologies in trade and commerce. The country's government has hailed the partnership as significant in its efforts to transition global trade from paper-based systems to digital platforms.

It also would yield savings in terms of time and operational cost as well as reduce propensity for fraud and human error, said ICC and Singapore government agency Infocomm Media Development Authority (IMDA) in a joint statement.

The 17 companies that signed up included manufacturer of pulp and paper products April Group, Japanese conglomerates Mitsubishi and Sumitomo, Hong Kong commodity trading company Noble Group, and Netherlands commodity trading company Trafigura Group. Singapore-owned companies including DBS Bank and PSA International also joined the partnership.

A global group representing more than 45 million companies, the ICC aims to promote international trade and responsible business conduct.

ICC's secretary-general John W.H Denton said: "Digital platforms will lower existing barriers to international trade in the coming years and enable many more businesses to participate in the new global economy. [ICC is] committed to enabling the broadest possible adoption of these digital technologies and support the development and recognition of universally accepted best practice standards for digitalisation, based on global consensus and the work being done by our partners today."

The announcement was made this week at the World Economic Forum in Davos, Switzerland, where Singapore's Minister for Communications and Information S. Iswaran spoke at the ICC Forum on "Taking Trade Digital". Noting that the Asian nation had spent the last 25 years establishing free trade agreements, he said such efforts now were expanded to include digital agreements.

Iswaran said the new partnership with ICC and the 17 organisations would establish the fundamentals to ensure trust in the digitalisation of trade, which he noted was a critical gap today. "Any effort to digitalise trade must support the multilateral rules-based system and enable interoperability," he added.

In this aspect, he said Singapore developed its TradeTrust framework to support "the trust element", so digital transactions could be conducted with confidence. The system focused on four main components, including the legal validity of digital documents, development of standards development to facilitate the interoperability and exchange of digital documents across systems, and an accreditation structure to certify technical applications that complied with relevant legislations. Underpinning the data flow was a public blockchain platform.

The development of TradeTrust is led by IMDA, alongside the Maritime Port Authority and Enterprise Singapore.

One of the first platforms built on the TradeTrust framework is ICC TradeFlow, which was jointly developed by ICC and trade tech company, Perlin, and in collaboration with IMDA, Trafigura, and DBS Bank.

A $20 million pilot trade was executed on the new platform last November with an iron ore shipment from South Africa to China. Partners involved in the pilot had made further major trade volume commitments to be executed on the platform.

Iswaran added that ICC's member base of 45 million companies potentially also could start tapping TradeFlow to conduct trade more efficiently.

The Singapore minister said: "The pilot TradeTrust saw documentation time reduced by more than half, from 45 to 20 days. Parties can now digitally map out trade instructions, track their execution, and more efficiently manage finance transactions... The more extensively companies use it, the stronger the value proposition is, because of the network effect."

Singapore earlier this week said it wrapped up negotiations with New Zealand and Chile on a digital economy pact that would cover various components, including digital identities, data flow, and artificial intelligence. The Digital Economy Partnership Agreement (DEPA) aimed to facilitate greater digital connectivity between the countries and establish multilateral rules on digital trade at the World Trade Organisation. The three nations would now work towards getting the agreement formally signed.

RELATED COVERAGE

Singapore, New Zealand, and Chile inch towards digital economy pact

Having wrapped up negotiations for the Digital Economy Partnership Agreement, which encompasses various components including digital identities, artificial intelligence, and digital trade, the three nations will now work to formally sign the agreement into force.

APAC nations pledge digital cooperation, but acknowledge some implementation challenging

Governments participating in the Asia-Pacific Telecommunity have laid out new five-year goals to "co-create a connected digital future" for the region that include the development of data privacy and cybersecurity policies and regulations, but admit that--given the number of countries involved--the rollout of some components will be challenging.

Singapore, Australia begin talks on digital economy pact

Trade agreement between both nations aims to drive 'greater connectivity' and bilateral economic relations, with cooperation touted to encompass several areas including e-payments, fintech, artificial intelligence (AI), and digital identity.

Singapore trade minister urges global 'integration' to drive tech innovation

Trade and Industry Minster Chan Chun Sing points to a "great challenge" today where several countries no longer support integration, putting the global industry at risk of becoming fragmented when companies such as Google, IBM, and PayPal rely on cross-border data flow for growth.

Singapore tax on overseas digital services kicks in tomorrow

Country's GST will be extended to include overseas digital services, including cloud storage, media subscription, and mobile apps, from January 1, 2020, with more than 100 providers of such services registered and slated to begin charging in the new year.