WHITE PAPER

Detecting and Preventing Rogue Devices

solarwinds

Detecting and Preventing Rogue Devices

We live in an IP-connected world. Within the span of two short decades, IP (Internet Protocol) has become the lingua franca of virtually all interconnected technology! Look around your desk. How many IP-connected devices do you see? Without a doubt, the synergy that comes from greater connectivity also creates greater challenges if you're an IT or security manager.

Network growth and complexity is skyrocketing. Before the explosion of IP-connected devices, networks typically grew with the number of connected users. However, now networks must scale three to five times for each employee based on the number of IP devices we use to do our work. This means the challenge of managing and securing endpoints has also become much more difficult.

Here, we'll take an in-depth look at some of the challenges of efficiently tracking endpoints, keeping your network safe from rogue devices, and then offer best practices for keeping everything safe and running at peak performance.

Before the explosion of IP-connected devices, networks typically grew with the number of users. However, now networks must scale 3x to 5x for each employee just to provide support for the many IP devices we use to do our work.

ROGUE RISK

When you consider all of the IP-connected devices on your network—PCs and laptops, VOIP phones, and "bring your own device" (BYOD) netbooks, tablets, smartphones and more—how many do you think you have? It's a fundamental question that needs to be answered. Without any indication, you can't adequately plan for capacity or manage the network to maximum efficiency. But there is also a deeper implication to this question. Often lurking out there are rogue devices that have the potential to cause harm to your network. The larger your network, the greater the potential risk. All it takes is one rogue device to wreak havoc. What is the economic cost to your company when operations come to a halt because "the network is down"? So what constitutes a rogue device and what can go wrong?

"BLACK HAT" ROGUE

By definition, rogue devices are just plain malicious in nature. They exist for the sole purpose of doing harm to your network and, in the process, to your reputation and career. They exist to steal information or to disrupt network operations. In rare cases, they can even permanently damage systems.

On the "most wanted" list of rogue devices are wireless access points (WAPs). A rogue WAP not only makes your network more porous but also circumvents your access controls. It's comparable to disabling the alarm and leaving the back door open.

Why do rogue WAPs pose such an inherent risk? By design, a WAP is a network bridge and is used to connect two disparate networks. (In this case, a wireless network to a wired network.) Wireless networks are inherently less secure than wired networks. With traditional (non-wireless) networks, data flows over physical and often-protected circuits. With wireless networks, data is instead transmitted using radio signals. This has several security implications. First, these signals can be intercepted, making data susceptible to eavesdropping. Second, a rogue WAP can open your network to unauthorized connections that are difficult to detect.

Rogue WAPs are particularly useful in perpetrating "man-in-the- middle" (MITM) attacks. A MITM attack is used to subvert trust between systems. For example, if I were to make an online transaction my computer would request authentication credentials (e.g., digital security certificate). By exchanging key credentials, both systems can "verify" each other's identity, establishing a level of privacy and trust. However, with a MITM attack the hacker, using a rogue WAP, would terminate my session with a valid WAP, and then fool my system into reconnecting through the rogue WAP. This puts the hacker "in the middle," or between my system and the system I want to transact with. Now one step removed from each other, when these systems attempt to authenticate, the hacker (in the middle) will send false credentials to both. The hacker authenticates with my system and with the transaction system. However, neither my system nor the transaction system authenticate directly with each other. Under this scenario each system believes it has established a level of trust with the other, when in reality both systems trust an untrustworthy system.

Rogue devices exist for the sole purpose of doing harm to your network and, in the process, to your reputation and career.

There are also variations of the MITM attack. In these instances, the rogue systems may intercept legitimate traffic and redirect it or change essential data by interjecting corrupted data into the exchange.

Beyond WAPs, there are other types of malicious rogue devices. These rogues include web robots (bots) and sniffers. A bot is a system that performs a repetitive task. Malicious bots can be used to send email spam or cause a network denial of service (DoS) condition. A DoS attack makes systems unavailable by creating conditions which result in the over-utilization of a system resulting in severe performance degradation. Bots can also be formed into a collective of "zombies" and used to perpetrate even more powerful attacks. And finally, there are sniffers. A sniffer is an "eavesdropper" that passively sits on the network and stealthily inspects traffic. Sniffers can be maliciously used for the reconnaissance of valuable data.

GOOD SYSTEMS GOING ROGUE

While rogue WAPs receive a lot of attention and discussion, we should not overlook the potential for trusted systems to permit rogue behavior. How? Here are few examples.

Endpoint Vulnerabilities

Trusted endpoints have inherent vulnerabilities in their operating systems and applications. These vulnerabilities can be exploited, giving hackers and forms of malware unrestricted access to your network.

Malfunctioning Hardware

In rare cases, malfunctioning hardware (think bad NIC) may cause network disruption. While technically not a malicious act, it nevertheless underscores the need to rapidly identify and quarantine offending systems.

BYOD Smartphones and Tablets

Consumer-oriented devices like smartphones and tablets are also invading corporate networks and creating unique risks and challenges. A factor that often complicates the smooth integration of BYOD devices into your network is that by their very nature of being consumer devices, they lack integration with IT management platforms. As a result, BYOD devices not only pose a risk to your network because of the sheer difficulty required to manage them, but also because of their susceptibility to malware and their propensity to consume valuable network resources.

From the preceding discussion, it should be apparent that anyone who has physical access to your network can do a great deal of damage. Therefore, it's vital that every reasonable effort be taken to secure your network access using both detection and prevention controls. So what can be done? Fortunately, quite a bit—and without investing a great deal of effort or expense. In the next section, we'll explore specific recommendations and steps you can take to help defend your network from these rogue devices.

DETECTING AND PREVENTING ROGUE DEVICES

Because your IP network is designed to provide distributed access, it's porous and intended to be accessible by many types of devices. Therefore, the objective of IT administrators is to limit access only to authorized devices.

When planning your prevention strategy, it's important to take a holistic approach. Technology alone will not completely address the problem and will require a combination of both procedural and technical controls. For this reason, many IT professionals turn to published standards to help guide them. One such standard is the ISO/ IEC 27002 standard. The recommendations that follow are derived from this standard. Appendix A contains a summary of selected controls used.

Physical Security

An unsecured, active RJ45 network jack or improperly configured WAP will provide easy access to your trusted network and is as good as a door left unlocked and propped open. It's almost like being able to enter your network from the internet by bypassing the firewall—unthinkable!

It may be difficult to gain physical access to a network through a secure data center. But it may be much easier to plug into an unsecured connection in the lobby or an unused office. An unsecured network connection is essential for connecting a sniffer or other rogue devices.

Therefore, your first line of defense will be to place a barrier around your network, which will restrict who can physically connect to your network infrastructure. This is done by controlling access to cabling and connection points. Physical security measures are typically incorporated into your facility and include special cabling conduits, locked work areas and equipment rooms. Obviously, it's important that these measures not be overlooked. Any failure in your physical security can yield the same effect as any other type of security breach that may result in unauthorized network access.

Your next line of defense will be to implement security controls at the network layer. The network layer represents the next logical area of vulnerability and point of incursion. To defend your network at this level, your objectives will be as follows:

1. Identify authorized devices
2. Build network access controls
3. Monitor network connected devices

Before we discuss each of these objectives in detail, it's important to understand that your network switches represent the best touch point for implementing many of these objectives. Why? Because your switches represent that part of your infrastructure which is in closest proximity to your network cabling. In addition, switches operate at OSI layers 1 and 2, and can detect activity on your network circuits which is not detectable at higher layers of network operations (e.g., OSI layers 3 through 7). (See appendix B for a primer on the OSI reference model.) As a result, they are much more capable at detecting connections to the network and are better equipped to perform asset identification, which can then be used for inventorying, access controls enforcement, and for supplying logging information used for monitoring and reporting purposes.

Identify Authorized Devices

Our first objective is to identify those devices (nodes and endpoints) that connect to the network. This information will then help us create device profiles and help us determine which devices are authorized. While there are many utilities that can be cobbled together to create a type of user device tracker, it will be a big time saver to use a centralized port monitoring tool that can combine the many steps and tasks and perform them across a variety of switches and devices located anywhere on your network. As we gather this information, we'll want to create a profile for each device that can document the following:

1. All switch and wireless access points nodes on your network
2. A profile for each node, including the owner's identification, contact information, physical location, summary performance, and capacity metrics
3. An inventory of all endpoint devices connection through this node device

Use Access Controls

Our second objective is to identify and verify which devices are authorized to use the network and to construct access controls using whitelists. Devices included in a whitelist will be able to connect to the network, whereas devices not whitelisted will not be permitted. Whitelists are a powerful tool. When used with a compatible port monitoring tool, you will be able to:

- Detect potential rogue devices and prevent them from accessing the network
- Revoke network access from a system that no longer conforms to your security policy
- Easily remove and quarantine an infected system from the network

Device Monitoring

Our third and final objective is to monitor network access for performance, capacity, including switch port capacity and compliance. When we monitor for compliance, we can refine our whitelists and ensure our controls are effective. When we monitor for performance, we can detect faults and errors that may affect performance and signal malicious activity. When we monitor for capacity, we can proactively avoid performance degradation and problems that typically occur as users try to augment the network with unauthorized hardware, software, or configuration changes.

As you implement these recommendations, remember to also integrate them with your operating procedures. For example, when you have changes in staffing, remember to update your whitelists. When you have network configuration changes, remember to update your device profiles. When you have incidents, make sure your response team is aware of these resources and capabilities.

There's one more thing to consider. Monitoring switches for whitelist compliance, switch performance and capacity is an essential start. However, more extensive monitoring can also yield important security dividends. If possible, you should also monitor activity on critical nodes and devices by using a Security Information and Event Management (SIEM) tool. This will allow you to detect anomalous behavior like irregular logins, permission escalations, and more. These types of events are often precursor attempts to exploit device vulnerabilities and turn a good system rogue. In addition, a SIEM solution will allow you to not only monitor systems, but also consolidate log data from multiple systems into a single event stream. This greatly expands your ability to detect exceptions across your entire operation, as opposed to doing this one system at a time. Also, a good log event monitor will allow you to create

rules, making it possible to correlate selected events from this consolidated event stream and detect complex intrusions. In addition, you'll want the ability to automate defensive actions by taking active responses if anomalous activity is detected—like issue an alert or terminate a connection. Lastly, when it comes to meeting and maintaining compliance with a variety of regulatory frameworks, an essential component involves the generation of reports that can help you demonstrate compliance to auditors. A good SIEM solution is not only also an essential component you need to strengthen your defenses, but also act in accordance with compliance regulations however they guide your strategy.

Use a port monitoring tool to save time. A good port monitor can combine the many steps and perform many required actions across a variety of switches and devices located anywhere on your network.

SUMMARY

Whether your organization has identified problems with rogue devices or not, the risks described in this paper are real. However, good IT security and management practices are not motivated by fear, but out of a sense of responsibility to protect the confidentiality, integrity, and availability of information assets. The recommendations provided not only present a policy-based approach to mitigate these risks, but also a baseline for helping to improve overall system security and integrity.

ABOUT USER DEVICE TRACKER (UDT)

SolarWinds User Device Tracker (UDT) delivers automated user and device tracking along with powerful switch port management capabilities so you can stay in control of who and what are connecting to your network. Quickly find a computer or user, as well as track down lost or rogue devices with a simple search on a user name, IP address, Hostname, or MAC address. And, if the user or device is no longer connected, historical data will show its last known location. You can even perform whitelisting or create a watch list, and be alerted immediately when a specific user or device connects. Plus, SolarWinds User Device Tracker lets you take immediate action to shut down a port and mitigate a threat or alleviate a network performance issue. Best of all, you can do it all from an easy-to-use, point-and-click web interface!

LEARN MORE **DOWNLOAD FREE TRIAL**

ABOUT LOG & EVENT MONITOR (LEM)

SolarWinds Log & Event Manager (LEM) delivers powerful Security Information and Event Management (SIEM) capabilities in a highly affordable, easy-to-deploy virtual appliance. It combines real-time log analysis, event correlation, and a groundbreaking approach to IT search to deliver the visibility, security, and control you need to overcome everyday IT challenges. SIEM software has never been easier to use or more affordable.

LEARN MORE **DOWNLOAD FREE TRIAL**

ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, THWACK, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.

APPENDIX A

The International Organization for Standardization (ISO) is an international, nongovernmental body that collaborates with the International Electrotechnical Commission (IEC) and the International Telecommunication Union for the purposes of publishing a body of standards for achieving effective management practices governing information security.

Elements of the ISO 27002 standard are widely adopted. They can be found in variant form in many vertical industry regulatory and governance standards including:

Companies conducting electronic commerce: Payment Card Industry Data Security Standard (PCI DSS)

Companies providing health care services: The Health Insurance Portability and Accountability Act (HIPPA)

Corporate Governance: Sarbanes-Oxley act (SOX), Gramm–Leach–Bliley Act (GLBA), Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), Committee of Sponsoring Organizations (COSO) and more.

US Government (and partners): Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS) Federal Information Processing Standards (NIST) and more.

Chances are, you're already using some elements of this standard at your company today.

The ISO 27002 standard establishes ten domains of focus including, but not limited to policy, asset management, physical security, operations management, access control, incident management and more. Furthermore, within each of these domains there are specific objectives and recommended technical and procedural controls, which should be implemented with discretion. In other words, the standard expresses what objectives should be achieved, but not the methods a company must use to achieve desired results. This gives organizations tremendous flexibility.

Coming back to that body of best practices that will help you detect and prevent rogue devices, the following are taken from the ISO 27002 Standard. When these objectives and controls are implemented and augmented with specialized tools, you can effectively defend against the effects of rogue devices on your network.

ISO 27002 DOMAIN	CONTROL & OBJECTIVE	APPLICABILITY	IDEAL USER DEVICE TRACKER/PORT MONITORING TOOL REQUIREMENTS
Security Policy	**5.1.1 Information security policy document.** An information security policy document should be approved by management, published, and communicated to all employees and relevant external parties.	Include provisions in your security policy which define and prohibit rogue devices.	
Organization of information security	**6.1.7 Contact with special interest groups.** Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	Learn proactively from peers about how they are managing problems with detecting and preventing rogue systems.	a) Provide knowledge about best practices and how to stay up to date with relevant information; b) share and exchange information about new technologies, products, threats, or vulnerabilities

ISO 27002 DOMAIN	CONTROL & OBJECTIVE	APPLICABILITY	IDEAL USER DEVICE TRACKER/PORT MONITORING TOOL REQUIREMENTS
Asset Management	**7.1.1 Inventory of assets.** All assets should be clearly identified and routinely inventoried.	Inventory of network assets helps to create awareness and ensure that uniform and effective asset protection.	Use discovery techniques to easily identify mixed-vendor devices.
Asset Management	**7.1.2 Ownership of assets.** All information and assets associated with information processing facilities should be owned by a designated part of the organization.	Establish who to contact when there's a problem with a switch or connected system.	Associate a profile with each device that includes owner, contact information, location, and logical groupings.
Human resources security	**8.3.2 Return of assets.** All employees, contractors, and third-party users should return all of the organization's assets in their possession upon termination of their employment, contract, or agreement.	Prevent good systems from "going rogue."	Remove systems unaccounted for from whitelists and create alerts if they connect to the network.
Human resources security	**8.3.3 Removal of access rights.** The access rights of all employees, contractors, and third-party users to information and information processing facilities should be removed upon termination of their employment, contract, or agreement, or adjusted upon change.	Prevent unused network jacks from being used for unauthorized purposes.	Easily deactivate physical network connections when not being used regardless of switch type and geographic location.
	PHYSICAL AND ENVIRONMENTAL SECURITY		
Communications and Operations Management	**10.3.1 Capacity management.** The use of resources should be monitored and tuned, and projections made of future capacity requirements to ensure the required system performance.	Eliminate the need for employees to "augment" the network with unauthorized devices.	Monitor switches for port, throughput utilization, and trends, regardless of vendor or geographic location.

ISO 27002 DOMAIN	CONTROL & OBJECTIVE	APPLICABILITY	IDEAL USER DEVICE TRACKER/PORT MONITORING TOOL REQUIREMENTS
Communications and Operations Management	**10.4.1 Controls against malicious code.** Establish detection, prevention, and recovery controls to protect against malicious code. Appropriate user awareness procedures should be implemented.	Isolate affected systems to prevent propagation and ensure remediated systems are ready to be reconnected to product environments.	Be able to easily quarantine a system or network segment in order to control the spread of malicious code over the network.
Communications and Operations Management	**10.10.1 Audit logging.** Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Begin/continue network access logging and monitoring to facilitate alerting and reporting.	Be able to easily consolidate switch logs, regardless of vendor or location, into one view. Be able to set alerts based on watch lists and create historical reports.
Communications and Operations Management	**10.10.5 Fault logging.** Faults should be logged, analyzed, and appropriate action then taken.	Monitor switch operations and log faults. Review faults for any indication of tampering.	Be able to easily consolidate switch logs, regardless of vendor or location, into one view. Be able to set alerts based on watch lists and create historical reports.
Access Control	**11.2 User access management.** Ensure authorized user access and to prevent unauthorized access to information systems. **11.4 Network access control.** Prevent unauthorized access to networked services.	Detect and prevent unauthorized systems from connecting to the network.	Centrally create and manage whitelists (authorized users), then monitor and alert on access by systems not “whitelisted,” regardless of switch type or location.

APPENDIX B

The OSI Model is a conceptual framework that defines how connected systems communicate. Using this model, professional associations and standards bodies have developed technical reference specifications (e.g., IEEE 802.3 [Ethernet]), IETF Transmission Control Protocol (TCP), Worldwide Web Consortium Hypertext Transfer Protocol [HTTP], etc.). In turn, vendors build products that conform to these technical reference specifications. When disparate systems conform to these specifications, they are able to communicate with each other.

Layer 1: Physical. These standards define the physical medium of communication. For machines, this means cable and pin standards, voltages, and other electrical specifications.

Layer 2: Data Link. These standards define how systems address, signal, encode, transmit, receive, and decode data with each other via the network. Essential characteristics of an Ethernet (IEEE 802.3) network are defined at this layer.

Layer 3: Network. These standards define how data is to be routed between systems that exist on different network segments. For a TCP/IP network, the essential Internet Protocol (IP) characteristics are defined at this layer.

Layer 4: Transport. These are services that ensure reliable communications between systems by introducing error detection and handling, flow control, and resend. For a TCP/IP network, the essential Transmission Control Protocol (TCP) characteristics are defined at this layer.

Layer 5: Session. These services are responsible for initiating, maintaining, and closing a dialogue between two computer systems.

Layer 6: Presentation. This layer transforms data, as needed, so it can be exchanged between two different systems. Examples of transformation that may occur at this level include bit order or encryption.

Layer 7: Application. This layer presents an end-user software application with an interface to network communication services. Examples of TCP/IP communication services include HTTP, FTP, SMTP, and SMTP