Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

August 2021

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

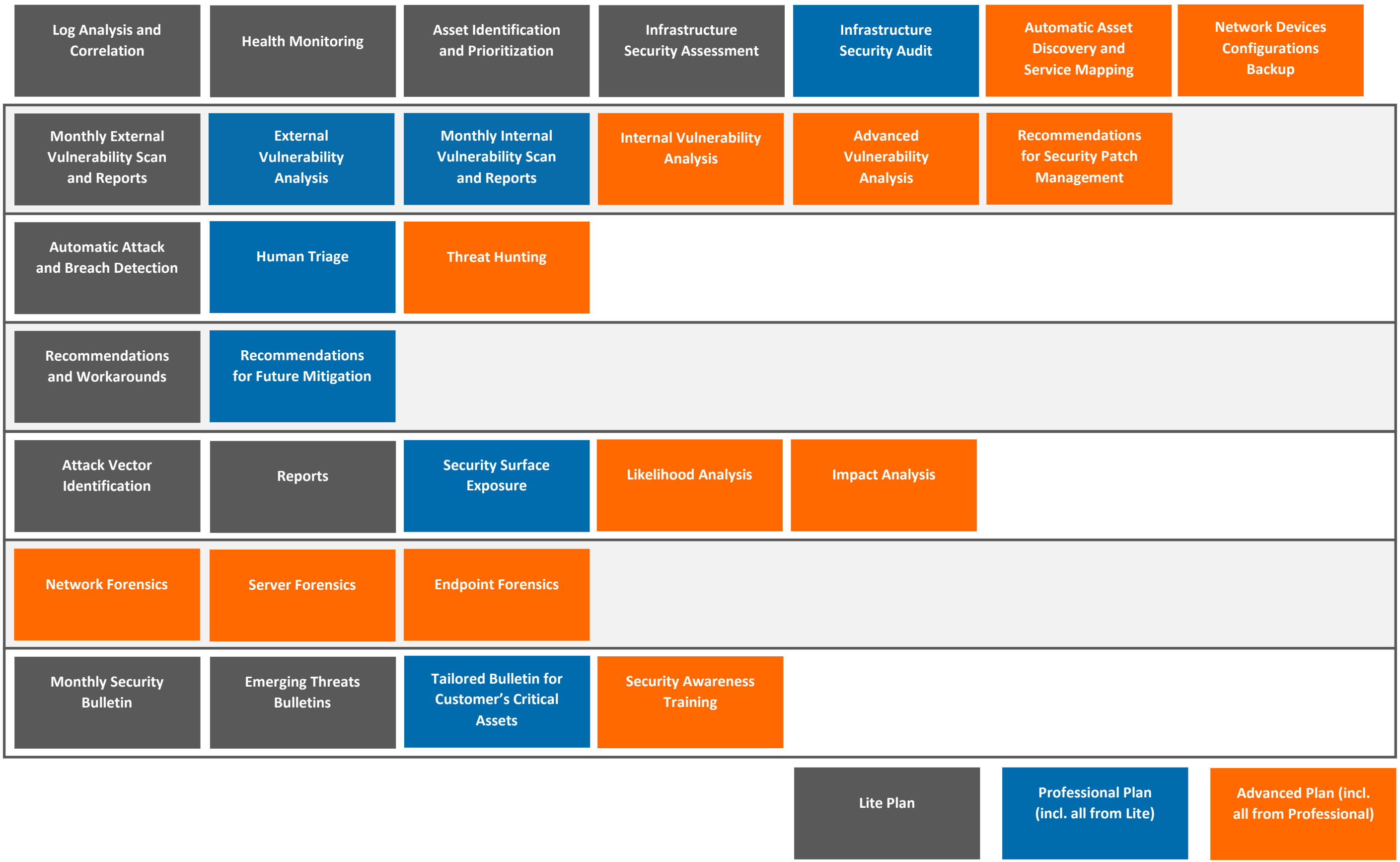
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!



⬛ Log Analysis and Correlation	⬛ Health Monitoring	⬛ Asset Identification and Prioritization	⬛ Infrastructure Security Assessment	🟦 Infrastructure Security Audit	🟧 Automatic Asset Discovery and Service Mapping	🟧 Network Devices Configurations Backup
⬛ Monthly External Vulnerability Scan and Reports	🟦 External Vulnerability Analysis	🟦 Monthly Internal Vulnerability Scan and Reports	🟧 Internal Vulnerability Analysis	🟧 Advanced Vulnerability Analysis	🟧 Recommendations for Security Patch Management	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and Workarounds	🟦 Recommendations for Future Mitigation					
⬛ Attack Vector Identification	⬛ Reports	🟦 Security Surface Exposure	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensics				
⬛ Monthly Security Bulletin	⬛ Emerging Threats Bulletins	🟦 Tailored Bulletin for Customer's Critical Assets	🟧 Security Awareness Training			

⬛ Lite Plan

🟦 Professional Plan (incl. all from Lite)

🟧 Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Netgear Authentication Bypass Allows Router Takeover 4
2. Microsoft: PrintNightmare security updates work, start patching! 5
3. Windows Hello Bypass Fools Biometrics Safeguards in PCs 7
4. Updated Joker Malware Floods into Android Apps 10
5. Linux version of HelloKitty ransomware targets VMware ESXi servers 12
6. 16-year-old bug in printer software gives hackers admin rights 14
7. New Windows 10 vulnerability allows anyone to get admin privileges 15
8. Critical Microsoft Hyper-V bug could haunt orgs for a long time 17
9. Google Play Protect fails Android security tests once more 19
10. Grief ransomware operation is DoppelPaymer rebranded 20
11. Novel Meteor Wiper Used in Attack that Crippled Iranian Train System 22
12. Amazon gets $888 million GDPR fine for behavioral advertising 24

1. Netgear Authentication Bypass Allows Router Takeover

Microsoft researchers discovered the firmware flaws in the DGN-2200v1 series router that can enable authentication bypass to take over devices and access stored credentials.

Microsoft security researchers discovered the bugs in Netgear DGN-2200v1 series routers while they were researching device fingerprinting, Microsoft 365 Defender research team's Jonathan Bar Or said in a blog post, posted Wednesday.

"We noticed a very odd behavior: A device owned by a non-IT personnel was trying to access a Netgear DGN-2200v1 router's management port," researchers wrote.

Researchers investigated and eventually identified the vulnerabilities, tracked as PSV-2020-0363, PSV-2020-0364 and PSV-2020-0365 by Netgear (CVEs were not issued), and which range in CVSS rating from high (7.4) to critical (9.4). They reported their discovery to Netgear, which has released a security advisory patching the flaws.

An attacker can exploit the flaws to breach a router's management pages without having to log in, and take over the router, as well as use a cryptographic side-channel attack to acquire the router's saved credentials, Bar wrote.

Full exploitation of the vulnerabilities "can compromise a network's security — opening the gates for attackers to roam untethered through an entire organization," he wrote.

Unpacking the Issue

Researchers downloaded the firmware for the device in question from Netgear's website to explore why there was a random device trying to connect with the router's management port. They observed that the anomalous communication used the standard port that HTTPd serves, so they chose to focus there to see where the problem might lie.

Researchers performed a static analysis of the HTTPd binary and dynamic analysis by running QEMU, an open-source emulator, among other tests to explore the issue, they said.

Eventually, while examining how HTTPd dictates which pages should be served without authentication, they found some "pseudo code" as the first page handling code inside HTTPd, automatically approving certain pages such as "form.css" or "func.js."

This in and of itself would not be a problem, Bar wrote, except "Netgear decided to use 'strstr' to check if a page has .JPG, .GIF or 'ess_' substrings, trying to match the entire URL," he said. This meant that researchers could access any page on the device, including those requiring authentication, "by appending a GET variable with the relevant substring (like '?.GIF")," he wrote.

Bar used the example “hxxps://10[.]0[.]138/WAN_wan.htm?pic.gif” to demonstrate how researchers achieved “a complete and fully reliable authentication bypass.” In this way, researchers achieved “complete control over the router,” he said.

Exploring Router Authentication

After that, researchers decided to dive even deeper to see how the authentication was implemented, finding that router credentials also could be gained using a side-channel attack, they said.

Moreover, they went on to use the first authentication-bypass vulnerability to see if they could recover the user name and password used by the router by another existing weakness, focusing on the device’s backup and restore feature. By reverse-engineering the functionality, they found that they could, Bar wrote.

“After some preparatory steps, the contents are DES-encrypted with a constant key ‘NtgrBak,'” he wrote. “This allows an attacker to get the plaintext password (which is stored in the encrypted NVRAM) remotely. The user name, which can very well be variations of ‘admin,’ can be retrieved the same way.”

“With this research, we have shown how a simple anomalous connection to a router, found through the endpoint discovery service, drove us to find several vulnerabilities on a popular router,” Bar wrote in the post. “Routers are integral to networking, so it is important to secure the programs supporting its functions.”

The vulnerabilities aren’t the first time Netgear routers have had authentication flaws, allowing attackers to use them as an entry point into the wider network. About a year ago researchers discovered an unpatched zero-day vulnerability in firmware that put 79 Netgear device models at risk for full takeover. Moreover, the company chose to leave 45 of those models unpatched because they were outdated or had reached their end of life.

Source: https://threatpost.com/netgear-authentication-bypass-router-takeover/167469/

2. Microsoft: PrintNightmare security updates work, start patching!

Microsoft says the emergency security updates released at the start of the week correctly patch the PrintNightmare Print Spooler vulnerability for all supported Windows versions and urges users to start applying the updates as soon as possible.

This clarified guidance comes after security researchers tagged the patches as incomplete after finding that the OOB security updates could be bypassed in specific scenarios.

"Our investigation has shown that the OOB security update is working as designed and is effective against the known printer spooling exploits and other public reports collectively being referred to as PrintNightmare," the Microsoft Security Response Center explains.

"All reports we have investigated have relied on the changing of default registry setting related to Point and Print to an insecure configuration."

Clarified PrintNightmare guidance

Microsoft has updated the PrintNightmare patch guidance and is now encouraging customers to update as soon as possible.

These are the correct steps required to patch this critical Windows Print Spooler RCE vulnerability as shared by Microsoft:

- In ALL cases, apply the CVE-2021-34527 security update. The update will not change existing registry settings

- After applying the security update, review the registry settings documented in the CVE-2021-34527 advisory

- If the registry keys documented do not exist, no further action is required

- If the registry keys documented exist, in order to secure your system, you must confirm that the following registry keys are set to 0 (zero) or are not present:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint

NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)

UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

Additional information and further guidance are available in the KB5005010 support document and the CVE-2021-34527 security advisory.

How to install the PrintNightmare security updates

You can find detailed steps on how to install these emergency security updates in the support documents linked below:

- Windows 10, version 21H1 (KB5004945)

- Windows 10, version 20H2 (KB5004945)

- Windows 10, version 2004 (KB5004945)

- Windows 10, version 1909 (KB5004946)

- Windows 10, version 1809 and Windows Server 2019 (KB5004947)

- Windows 10, version 1607 and Windows Server 2016 (KB5004948)

- Windows 10, version 1507 (KB5004950)

- Windows Server 2012 (Monthly Rollup KB5004956 / Security only KB5004960)

- Windows 8.1 and Windows Server 2012 R2 (Monthly Rollup KB5004954 / Security only KB5004958)

- Windows 7 SP1 and Windows Server 2008 R2 SP1 (Monthly Rollup KB5004953 / Security only KB5004951)

- Windows Server 2008 SP2 (Monthly Rollup KB5004955 / Security only KB5004959)

If you cannot immediately install the security updates on your system(s), you can disable the Windows Print Spooler service to mitigate the PrintNightmare vulnerability temporarily.

Thursday night, Microsoft has also issued an emergency fix to address printing issues affecting Zebra and Dymo receipt or label printers due to changes introduced in the June 2021 cumulative update preview with the recently released KB5003690, KB5004760, and KB5004945 updates.

This fix is being rolled out via Microsoft's Known Issue Rollback (KIR) feature, which pushes fixes for known issues through Windows Update and should reach most impacted systems within 24 hours (restarting the computer may also speed up the process.)

Source: https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-security-updates-work-start-patching/

3. Windows Hello Bypass Fools Biometrics Safeguards in PCs

A Windows security bug would allow an attacker to fool a USB camera used in the biometric facial-recognition aspect of the system.

A vulnerability in Microsoft’s Windows 10 password-free authentication system has been uncovered that could allow an attacker to spoof an image of a person’s face to trick the facial-recognition system and take control of a device.

Windows Hello is a feature in Windows 10 that allows users to authenticate themselves without a password, using a PIN code or biometric identity—either a fingerprint or facial recognition—to access a device or machine. According to Microsoft, about 85 percent of Windows 10 users use the system.

The Windows Hello bypass vulnerability, tracked as CVE-2021-34466, requires an attacker to have physical access to a device to exploit it, according to researchers at CyberArk Labs who discovered the flaw in March.

From there, they can go on "to manipulate the authentication process by capturing or recreating a photo of the target's face and subsequently plugging in a custom-made USB device to inject the spoofed images to the authenticating host," Omer Tsarfati, cybersecurity researcher at CyberArk Labs, wrote in a report about the vulnerability published Tuesday.

Further, exploitation of the bypass can extend beyond Windows Hello systems to "any authentication system that allows a pluggable third-party USB camera to act as biometric sensor," Tsarfati noted.

Researchers have no evidence that anyone has tried or used the attack in the wild, but someone with motive could potentially use it on a targeted espionage victim, such as "a researcher, scientist, journalist, activist or privileged user with sensitive IP on their device, for example," according to the analysis.

Microsoft addressed the vulnerability — which affects both consumer and business versions of the feature — in its July Patch Tuesday update. Also, Windows users with Windows Hello Enhanced Sign-in Security — a new security feature in Windows that requires specialized and pre-installed hardware, drivers and firmware — are protected against the any attacks "which tamper with the biometrics pipeline," according to Microsoft.

However, Tsarfati said that the solution may not fully mitigate the issue.

"Based on our preliminary testing of the mitigation, using Enhanced Sign-in Security with compatible hardware limits the attack surface but is dependent on users having specific cameras," he said. "Inherent to system design, implicit trust of input from peripheral devices remains. To mitigate this inherent trust issue more comprehensively, the host should validate the integrity of the biometric authentication device before trusting it."

Biometric Weakest Link

CyberArk researchers posted a video of a proof-of-concept (PoC) for how to exploit the vulnerability, which can be used on both the consumer version, Windows Hello, and an enterprise version of the feature called Windows Hello for Business (WHfB) that businesses use with ActiveDirectory.

The bypass itself exploits a weakness in the biometric sensor of Windows Hello, which "transmits information on which the OS … makes its authentication decision," he wrote. "Therefore, manipulating this information can lead to a potential bypass to the whole authentication system," Tsarfati said.

For facial recognition, the biometric sensor is either a camera embedded in a device, such as a laptop, or connected to a computer via USB. Therefore, the entire process depends on this camera for proof of identity–which is where the vulnerability lies, particularly when a USB camera is used for authentication, he wrote.

"The answer lies in the input itself," Tsarfati wrote. "Keyboard input is known only to the person who is typing before the information is entered into the system, while camera input isn't."

Therefore, using a camera to access "public" information—i.e., a person's face—for authentication can easily be hijacked, he explained.

"It is similar to stealing a password, but much more accessible since the data (face) is out there," Tsarfati wrote. "At the heart of this vulnerability lies the fact that Windows Hello allows external data sources, which can be manipulated, as a root of trust."

Attack Vector

Researchers detailed a somewhat complex way for an attacker to capture someone's image, save the captured frames, impersonate a USB camera device, and eventually send those frames to the Windows hello system for verification.

To prove the concept, they created a custom USB device that acts as a USB camera with both infrared (IR) and Red Green Blue (RGB) sensors, using an evaluation board manufactured by NXP. They used this custom camera to transmit valid IR frames of the person they were targeting, while sending the RGB frames image of the cartoon character SpongeBob SquarePants.

"To our surprise, it worked!" Tsarfati wrote.

Based on this understanding, an attacker would only need to implement a USB camera that supports RGB and IR cameras and then send only one genuine IR frame of a victim to bypass the login phase of the device, while the RGB frames can contain any random image, he explained.

The entire process depends on an attacker having an IR frame of a potential victim to use in an attack, which can be done either by capturing one or converting one of the person's regular RBG frames to an IR one, Tsarfati explained.

"Our findings show that any USB device can be cloned, and any USB device can impersonate any other USB device," he said. "We used the IR frames of a person to 'bypass' the face recognition mechanism. We believe that those IR frames can be created out of regular color images."

Source: https://threatpost.com/windows-hello-bypass-biometrics-pcs/167771/

4. Updated Joker Malware Floods into Android Apps

The Joker premium billing-fraud malware is back on Google Play in a fresh onslaught, with an updated bag of tricks to evade scanners.

The Joker mobile trojan is back on Google Play, with an uptick in malicious Android applications that hide the billing-fraud malware, researchers said. It's also using new approaches to skirt past Google's app-vetting process.

Joker has been around since 2017, disguising itself within common, legitimate apps like camera apps, games, messengers, photo editors, translators and wallpapers. Once installed, Joker apps silently simulate clicks and intercept SMS messages to subscribe victims to unwanted, paid premium services controlled by the attackers – a type of billing fraud that researchers categorize as "fleeceware." The apps also steal SMS messages, contact lists and device information. Often, the victim is none the wiser until the mobile bill arrives.

Malicious Joker apps are commonly found outside of the official Google Play store, but they've continued to skirt Google Play's protections since 2019 too. That's mostly because the malware's authors keep making small changes to their attack methodology. As a result, there have been periodic waves of Joker infestations inside the official store, including two massive onslaughts last year. According to researchers at Zimperium, more than 1,800 Android applications infected with Joker have been removed from the Google Play store in the last four years.

In the latest wave, at least 1,000 new samples have been detected just since September, many of them finding their way into the official marketplace, researchers said.

"Malicious actors have routinely found new and unique ways to get this malware into both official and unofficial app stores," according to a Zimperium analysis, posted Tuesday. "While they are never long for life in these repositories, the persistence highlights how mobile malware, just like traditional endpoint malware, does not disappear but continues to be modified and advanced in a constant cat-and-mouse game."

Legitimate Developer Techniques

The developers of the latest versions of Joker, which began emerging in late 2020, are taking advantage of legitimate developer techniques to "try and hide the actual intent of the payload from traditional, legacy-based mobile security toolsets," according to Zimperium — which helps them evade both device-based security and app store protections.

One way they're doing that is to use Flutter, which is an open-source app development kit designed by Google that allows developers to craft native apps for mobile, web and desktop from a single codebase. The use of Flutter to code mobile applications is a common approach, and one that traditional scanners see as benign.

"Due to the commonality of Flutter, even malicious application code will look legitimate and clean, whereas many scanners are looking for disjointed code with errors or improper assemblies," explained the researchers.

Other New Tricks in the Bag

According to the analysis, another anti-detection technique lately adopted by Joker enthusiasts is the practice of embedding the payload as a .DEX file that can be obfuscated in different ways, such as being encrypted with a number, or hidden inside an image using steganography. Sometimes in the latter case, the image is hosted in legitimate cloud repositories or on a remote command-and-control (C2) server, researchers said.

Other new behavior includes using URL shorteners to hide the C2 addresses, and using a combination of native libraries to decrypt an offline payload.

Researchers said that the new samples also take extra precautions to remain hidden after a trojanized app is installed.

"After successful installation, the application infected with Joker will run a scan using Google Play APIs to check the latest version of the app in Google Play Store," they explained. "If there is no answer, the malware remains silent since it can be running on a dynamic analysis emulator. But if the version found in the store is older than the current version, the local malware payload is executed, infecting the mobile device. If the version in the store is newer than the current one, then the C2s are contacted to download an updated version of the payload."

No Joke: Consumers and Enterprises Alike at Risk

The apps are cropping up not only in Google Play and unofficial third-party markets, but also in other sanctioned outlets, some for the first time. For instance, AppGallery – the official app store for Huawei Android – was recently found to be infested with apps that contained the Joker trojan. According to Doctor Web back in April, the apps were downloaded by unwitting users to more than 538,000 devices.

"Sadly, the Joker malware is no joke," Saryu Nayyar, CEO at Gurucul, said via email. "And even more depressing, no dark knight is going to ride in to save users from these malicious apps. Users have to manually clean their devices of this pesky malware. The good news is that it appears the only damage is financial, and likely temporary. Users who have been subscribed to premium mobile services as a result of this malware can request refunds for said services since the affected applications are known."

Josh Bohls, CEO and founder at Inkscreen, noted earlier in the year that Joker is also a problem for companies, not just individuals.

"These malicious applications can find their way into the enterprise when an infected device is enrolled in a company's bring-your-own-device (BYOD) program, and suddenly you have a new threat vector," he said via email. "We hope to see better app review processes by Apple and Google, and that consumer and business buyers continue to educate themselves on how to select appropriate mobile applications."

Source: https://threatpost.com/updated-joker-malware-android-apps/167776/

5. Linux version of HelloKitty ransomware targets VMware ESXi servers

The ransomware gang behind the highly publicized attack on CD Projekt Red uses a Linux variant that targets VMware's ESXi virtual machine platform for maximum damage.

As the enterprise increasingly moves to virtual machines for easier backup and resource management, ransomware gangs are evolving their tactics to create Linux encryptors that target these servers.

VMware ESXi is one of the most popular enterprise virtual machine platforms. Over the past year, there has been an increasing number of ransomware gangs releasing Linux encryptors targeting this platform.

While ESXi is not strictly Linux as it uses its own customer kernel, it does share many similar characteristics, including the ability to run ELF64 Linux executables.

HelloKitty moves to ESXi

Yesterday, security researcher MalwareHunterTeam found numerous Linux ELF64 versions of the HelloKitty ransomware targeting ESXi servers and the virtual machines running on them.

It has been known that HelloKitty utilizes a Linux encryptor, but this is the first sample that researchers have publicly spotted.

Ransomware gangs targeting ESXi servers will shut down virtual machines before encrypting files to prevent the files from being locked and to avoid data corruption.

When shutting down the virtual machines, the ransomware will first try a graceful shutdown using the 'soft' command:

- esxcli vm process kill -t=soft -w=%d

If there are still VMs running, it will try an immediate shutdown of virtual machines using the 'hard' command:

- esxcli vm process kill -t=hard -w=%d

Finally, if virtual machines are still running, the malware will use the 'force' command to shut down any running VMs forcefully.

- esxcli vm process kill -t=force -w=%d

After the virtual machines are shut down, the ransomware will begin encrypting .vmdk (virtual hard disk), .vmsd (metadata and snapshot information), and .vmsn (contains the active state of the VM) files.

This method is very efficient as it allows a ransomware gang to encrypt many virtual machines with a single command.

Last month, MalwareHunterTeam also found a Linux version of the REvil ransomware that targets ESXi servers and used the esxcli command as part of the encryption process.

Emsisoft CTO Fabian Wosar told BleepingComputer at the time that other ransomware operations, such as Babuk, RansomExx/Defray, Mespinoza, GoGoogle, and the now-defunct DarkSide, have also created Linux encryptors to target ESXi virtual machines.

"The reason why most ransomware groups implemented a Linux-based version of their ransomware is to target ESXi specifically," said Wosar.

A bit about HelloKitty

HelloKity has been in operation since November 2020, when a victim first posted about the ransomware in our forums.

Since then, the threat actors have not been particular actively compared to other human-operated ransomware operations.

Their most well-known attack has been against CD Projekt Red, where the threat actors encrypted devices and claim to have stolen source code for Cyberpunk 2077, Witcher 3, Gwent, and more.

The threat actors later claimed that someone had purchased the files stolen from CD Projekt Red.

This ransomware, or its variants, has been used under different names such as DeathRansom and Fivehands.

Source: https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/

6. 16-year-old bug in printer software gives hackers admin rights

A 16-year-old security vulnerability found in HP, Xerox, and Samsung printers drivers allows attackers to gain admin rights on systems using the vulnerable driver software.

"This high severity vulnerability, which has been present in HP, Samsung, and Xerox printer software since 2005, affects hundreds of millions of devices and millions of users worldwide," according to a SentinelOne report published today and shared with BleepingComputer in advance.

The security flaw tracked as CVE-2021-3438 is a buffer overflow in the SSPORT.SYS driver for specific printer models that could lead to a local escalation of user privileges.

As the researchers discovered, the buggy driver automatically gets installed with the printer software and will be loaded by Windows after each system reboot.

This makes it the perfect target for attackers who need an easy way to escalate privileges, since the bug can be abused even when the printer is not connected to the targeted device.

Successful exploitation requires local user access which means that threat actors will need to first get a foothold on the targeted devices.

Once this is achieved, they can abuse the security bug to escalate privileges in low complexity attacks without requiring user interaction.

The result is that attackers with basic user privileges can elevate their privileges to SYSTEM and run code in kernel mode, potentially bypassing security products that would block their attacks or the delivery of additional malicious payloads.

"Successfully exploiting a driver vulnerability might allow attackers to potentially install programs, view, change, encrypt or delete data, or create new accounts with full user rights," SentinelOne explains.

"While we haven't seen any indicators that this vulnerability has been exploited in the wild up till now, with hundreds of millions of enterprises and users currently vulnerable, it is inevitable that attackers will seek out those that do not take the appropriate action."

Users urged to update ASAP

A list of affected printer models using the vulnerable driver can be found in HP's security advisory and this Xerox security mini bulletin.

HP, Xerox, and Samsung enterprise and home customers are urged to apply the patches provided by the two vendors as soon as possible.

"Some Windows machines may already have this driver without even running a dedicated installation file, since this driver comes with Microsoft Windows via Windows Update," the researchers added.

Earlier this year, SentinelOne researchers found a 12-year-old privilege escalation bug in Microsoft Defender Antivirus (formerly Windows Defender) that can let attackers gain admin rights on unpatched Windows systems.

Microsoft Defender Antivirus is the default anti-malware solution on more than 1 billion systems running Windows 10 per Microsoft's stats.

Source: https://www.bleepingcomputer.com/news/security/16-year-old-bug-in-printer-software-gives-hackers-admin-rights/

7. New Windows 10 vulnerability allows anyone to get admin privileges

Windows 10 and Windows 11 are vulnerable to a local elevation of privilege vulnerability after discovering that users with low privileges can access sensitive Registry database files.

The Windows Registry acts as the configuration repository for the Windows operating system and contains hashed passwords, user customizations, configuration options for applications, system decryption keys, and more.

The database files associated with the Windows Registry are stored under the C:\Windows\system32\config folder and are broken up into different files such as SYSTEM, SECURITY, SAM, DEFAULT, and SOFTWARE.

As these files contain sensitive information about all user accounts on a device and security tokens used by Windows features, they should be restricted from being viewed by regular users with no elevated privileges.

This is especially true for the Security Account Manager (SAM) file as it contains the hashed passwords for all users on a system, which threat actors can use to assume their identity.

SAM file can be read by anyone

Yesterday, security researcher Jonas Lykkegaard told BleepingComputer he discovered that the Windows 10 and Windows 11 Registry files associated with the Security Account Manager (SAM), and all other Registry databases, are accessible to the 'Users' group that has low privileges on a device.

These low permissions were confirmed by BleepingComputer on a fully patched Windows 10 20H2 device, as shown below.

With these low file permissions, a threat actor with limited privileges on a device can extract the NTLM hashed passwords for all accounts on a device and use those hashes in pass-the-hash attacks to gain elevated privileges.

As the Registry files, such as the SAM file, are always in use by the operating system, when you attempt to access the file, you will receive an access violation as the files are open and locked by another program.

However, as the Registry files, including the SAM, are usually backed up by the Windows shadow volume copies, Lykkegaard says you can access the files through shadow volumes without an access violation.

For example, threat actors can use the following Win32 device namespace path for shadow volume copies below to access the SAM file by any user on the computer.

Using these low and incorrect file permissions, along with shadow volume copies of the files, Security researcher and Mimikatz creator Benjamin Delpy has told BleepingComputer that you could easily steal an elevated account's NTLM hashed password to gain higher privileges.

In addition to stealing NTLM hashes and elevating privileges, Delpy told BleepingComputer that this low privileged access could allow for further attacks, such as Silver Ticket attacks.

It is unclear why Microsoft changed the permissions on the Registry to allow regular users to read the files.

However, Will Dormann, a vulnerability analyst for CERT/CC, and SANS author Jeff McJunkin, said Microsoft introduced the permission changes in Windows 10 1809.

Strangely, Dormann stated that when installing a fresh version of Windows 10 20H2 from June, the loose permissions were not present.

Therefore, it is not clear if Microsoft fixed the permission issue when performing a clean. installation of Windows but did not fix it when upgrading to new versions.

Microsoft confirms vulnerability

In a security advisory released today, Microsoft has confirmed the vulnerability and is now tracking it as CVE-2021-36934.

"We are investigating and will take appropriate action as needed to help keep customers protected," Microsoft told BleepingComputer.

Security researchers are also =referring to this vulnerability as 'SeriousSAM' or 'HiveNightmare.'

In the advisory, Microsoft has shared mitigations that restrict the permissions on the C:\Windows\system32\config folder.

To block exploitation of this vulnerability temporarily you need to take the following steps:

Restrict access to the contents of %windir%\system32\config:

1 - Open Command Prompt or Windows PowerShell as an administrator.

2 - Run this command: icacls %windir%\system32\config\*.* /inheritance:e

Delete Volume Shadow Copy Service (VSS) shadow copies:

1 - Delete any System Restore points and Shadow volumes that existed prior to restricting access to %windir%\system32\config.

2 - Create a new System Restore point (if desired).

Source: https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/

8. Critical Microsoft Hyper-V bug could haunt orgs for a long time

Technical details are now available for a vulnerability that affects Hyper-V, Microsoft's native hypervisor for creating virtual machines on Windows systems and in Azure cloud computing environment.

Currently tracked as CVE-2021-28476, the security issue has a critical severity score of 9.9 out of 10. Exploiting it on unpatched machines can have a devastating impact as it allows crashing the host (denial of service) or execute arbitrary code on it.

Terminate VMs or take full control

The bug is in Hyper-V's network switch driver (vmswitch.sys) and affects Windows 10 and Windows Server 2012 through 2019. It emerged in a build from August 2019 and received a patch earlier this year in May.

Public details about the flaw are scarce at the moment but in a blog post today, researchers Peleg Hadar of SafeBreach and Ophir Harpaz of Guardicore explain where the fault is and why it is exploitable. The two researchers found the bug together and disclosed it privately to Microsoft.

The flaw stems from the fact that Hyper-V's virtual switch (vmswitch) does not validate the value of an OID (object identifier) request that is intended for a network adapter (external or connected to vmswitch).

An OID request can include hardware offloading, Internet Protocol security (IPsec), and single root I/O virtualization (SR-IOV) requests.

"While processing OID requests, vmswitch traces their content for logging and debugging purposes; this also applies to OID_SWITCH_NIC_REQUEST. However, due to its encapsulated structure, vmswitch needs to have special handling of this request and dereference OidRequest to trace the inner request as well. The bug is that vmswitch never validates the value of OidRequest and can thus dereference an invalid pointer," Harpaz explains

An attacker successfully leveraging this vulnerability needs to have access to a guest virtual machine (VM) and send a specially crafted packet to the Hyper-V host.

The result can be either crashing the host - and terminate all the VMs running on top of it, or gaining remote code execution on the host, which gives complete control over it and the attached VMs.

Orgs are slow to patch

While the Azure service is safe from this issue, some local Hyper-V deployments are likely still vulnerable as not all admins update Windows machines when patches come out.

Harpaz told BleepingComputer that vulnerabilities that remain unpatched for years on machines in enterprise networks are a common encounter for Guardicore.

One of the most common examples is EternalBlue that became known in April 2017 - patched a month earlier and leveraged in the destructive WannaCry and NotPetya cyberattacks.

"There are so many Windows Servers today that are vulnerable to well-known bugs, I won't be surprised if this bug stays unpatched for a very long time in organizations" - Ophir Harpaz

Harpaz and Hadar are scheduled for a presentation at the Black Hat security conference on August 4 on their research and how found the vulnerability using an in-house fuzzing program called hAFL1.

Source: https://www.bleepingcomputer.com/news/security/critical-microsoft-hyper-v-bug-could-haunt-orgs-for-a-long-time/

9. Google Play Protect fails Android security tests once more

Google Play Protect, the Android built-in malware defense system, has failed the real-world tests of antivirus testing lab AV-TEST after detecting just over two thirds out of more than 20,000 malicious apps it was pitted against.

Google's Android mobile threat protection, which automatically scans over 100 billion apps every day, was introduced during the Google I/O 2017 in May 2017, with rollout to all Android devices starting in July 2017.

Since then, Google Play Protect has been deployed to billions of devices and is now the built-in malware protection on over 2.5 billion active Android devices.

According to AV-TEST's results, Google's mobile threat protection solution ranked last out of 15 Android security apps tested over a span of six months, between January to June 2021.

While always running and scanning every app installed and launched on the device, "the endurance test revealed that this service does not provide particularly good security: every other security app offers better protection than Google Play Protect."

During this 5-month long endurance test, Google Play Protect detected a little over two-thirds of nearly 20,000 infected apps the testing lab used as part of three rounds of tests.

Each of these testing rounds pitted the security apps against over 3,000 newly-discovered malware samples (up to 24 hours old) and a reference set of more than 3,000 other up to one-month-old samples.

"A total of 5 apps always detected all the attackers 100 percent in the real-time test and in the test with the reference set," AV-TEST found.

"Finishing in last place, Google Play Protect only detected 68.8 percent in the real-time test and 76.6 percent in the test with the reference set."

Out of all mobile security apps tested, Bitdefender, G DATA, McAfee, NortonLifeLock, and Trend Micro were the ones that hit a perfect 100% detection rate.

Google Play Protect also mistakenly detected 70 apps as potentially malicious out of almost 10,000 harmless ones installed by AV-TEST from the Play Store and third-party Android app stores.

Given that the Android built-in malware protection solution failed to detect over a third of the 20,000 malware samples thrown at it during the tests, AV-TEST advises users to use a second security app to block malware slipping through Play Protect's defenses.

Last year, Google Play Protect also scored zero out of six points in Android protection tests but, this time, detecting only 37% of 3,300 newly discovered samples (up to 24 hours old) and 33.1% of those from the reference set of 3,300 malware samples (circulating for up to 4 weeks).

One year earlier, Google joined efforts with ESET, Lookout, and Zimperium to establish the App Defense Alliance as part of an effort to improve Android malware detection on submission and block malicious apps before getting published on the Play Store.

BleepingComputer has reached out to Google for comment on AV-TEST's results but had not heard back at the time of this publication.

Source: https://www.bleepingcomputer.com/news/security/google-play-protect-fails-android-security-tests-once-more/

10. Grief ransomware operation is DoppelPaymer rebranded

After a period of little to no activity, the DoppelPaymer ransomware operation has made a rebranding move, now going by the name Grief (a.k.a. Pay or Grief).

It is unclear if any of the original developers are still behind this ransomware-as-a-service (RaaS) but clues uncovered by security researchers point to a continuation of the “project.”

DoppelPaymer’s activity started to decline in mid-May, about a week after DarkSide ransomware’s attack on Colonial Pipeline, one of the largest fuel pipeline operators in the U.S.

With no updates on their leak site since May 6, it looked like the DoppelPaymer gang was taking a step back, waiting for the public’s attention to ransomware attacks to dissipate.

However, security researchers last month pointed that Grief and DoppelPaymer were names for the same threat.

Fabian Wosar of Emsisoft told BleepingComputer that the two shared the same encrypted file format and used the same distribution channel, the Dridex botnet.

Despite the threat actor’s effort to make Grief look like a separate RaaS, the similarities to DoppelPaymer are so striking that a connection between the two is impossible to dismiss.

News about Grief ransomware emerged in early June, when it was believed to be a new operation but a sample was found with a compilation date of May 17.

Malware researchers at cloud security company Zscaler analyzed the early Grief ransomware sample and noticed that the ransom note dropped on infected systems pointed to the DoppelPaymer portal.

“This suggests that the malware author may have still been in the process of developing the Grief ransom portal. Ransomware threat groups often rebrand the name of the malware as a diversion” - Zscaler

The connection between the two extends further, to their leak sites. Although visually they could not be more different, similarities abound, like the captcha code that prevents automated crawling of the site.

Furthermore, the two ransomware threats rely on highly similar code that implements “identical encryption algorithms (2048-bit RSA and 256-bit AES), import hashing, and entry point offset calculation.”

Another similarity is that both Grief and DoppelPaymer use the European Union General Data Protection Regulation (GDPR) as a warning that non-paying victims would still have to face legal penalties due to the breach.

There is so little setting the two apart, and it’s mostly cosmetic, that malware researchers strongly believe that it’s the same operation under a different name.

For instance, Grief switched to Monero cryptocurrency, which could be a protective measure against potential action from law enforcement that could lead to seizing the ransom money already collected.

Another difference is that Grief ransomware uses the term “griefs” for the victim data leaked on their site either as proof of the compromise (“griefs in progress”) or as punishment for not paying the ransom (“complete griefs”).

At the moment, there are more than two dozen victims listed on the Grief leak site, showing that the threat actor has been busy working under the new name. It looks like the gang also claims the recent attack on the Greek city Thessaloniki, publishing a file archive as proof of the intrusion.

Zscaler says that “Grief ransomware is the latest version of DoppelPaymer ransomware with minor code changes and a new cosmetic theme,” adding that the gang has kept in the shadow to avoid the level of attention that REvil got for breaching Kaseya and DarkSide for hitting Colonial Pipeline.

A ransomware gang rebranding is not necessarily looking to erase their tracks and may be doing it to avoid any government sanctions that would prevent victims from paying the ransom.

A short list of five hashes for the samples that Zscaler caught is available in the blog post.

Source: https://www.bleepingcomputer.com/news/security/grief-ransomware-operation-is-doppelpaymer-rebranded/

11. Novel Meteor Wiper Used in Attack that Crippled Iranian Train System

A July 9th attack disrupted service and taunted Iran's leadership with hacked screens directing customers to call the phone of Iranian Supreme Leader Khamenei with complaints.

An attack earlier this month on Iran's train system, which disrupted rail service and taunted Iran's leadership via hacked public transit display screens, used a never-before-seen wiper malware called Meteor that appears to have been design for reuse, a security researcher has found.

The initial attack, dubbed MeteorExpress, occurred July 9, when "a wiper attack paralyzed the Iranian train system," according to a report by Juan Andres Guerrero-Saade at Sentinel Systems.

That attack disrupted service and directed customers via all of the displays and message boards at the train station to call "64411"–the number for the office of Supreme Leader Ali Khamenei—for more information.

The next day, attackers also hit the website and computer systems of the staff of Iran's the Ministry of Roads and Urban Development, according to a published report.

SentinelLabs researchers reconstructed most of the attack chain in the train-system and discovered the novel wiper, which the threat actors—who also appear to be a new set of adversaries still finding their attack rhythm–refer to as Meteor, Guerrero-Saade wrote.

Guerrero-Saade credited security researcher Anton Cherepanov with identifying an early analysis of the event written in Farsi by an Iranian antivirus company as helping researchers recreate the attack.

What they discovered is that "behind this outlandish tale of stopped trains and glib trolls" are "the fingerprints of an unfamiliar attacker," using a wiper that "was developed in the past three years and was designed for reuse," Guerrero-Saade wrote.

Reconstructing the Attack

Overall, the toolkit that orchestrated the attack was comprised of a combination of batch files that implemented different components dropped from RAR archives, according to SentinelLabs. Attackers used the batch files, nested alongside their respective components, in a chain to successfully execute the attack.

“The wiper components are split by functionality: Meteor encrypts the filesystem based on an encrypted configuration, nti.exe corrupts the MBR, and mssetup.exe locks the system,” Guerrero-Saade wrote.

Researchers recovered “a surprising amount of files” for a wiper attack, but did not manage to reconstruct them all. One missing notable component was the MBR corrupter, nti.exe; its absence is significant because files overwritten by this component are the same as those overwritten by the notorious NotPetya ransomware, which crippled organizations around the world in 2017, Guerrero-Saade noted.

Despite the attack’s success, however, researchers found “a strange level of fragmentation to the overall toolkit,” he said.

“Batch files spawn other batch files, different RARarchives contain intermingled executables, and even the intended action is separated into three payloads: Meteor wipes the filesystem, mssetup.exe locks the user out, and nti.exe presumably corrupts the MBR,” Guerrero-Saade wrote.

Specific Attack Components

Researchers identified and elaborated two of those three payloads in the report. One is the main payload, the Meteor wiper, which comes in the form of an executable dropped under env.exe or msapp.exe,and is executed as a scheduled task with a single argument– an encrypted JSON configuration file, msconf.conf, that holds values for corresponding keys contained in cleartext within the binary, according to the report.

“At its most basic functionality, the Meteor wiper takes a set of paths from the encrypted config and walks these paths, wiping files,” Guerrero-Saade wrote. “It also makes sure to delete shadow copies and removes the machine from the domain to avoid means of quick remediation.”

The wiper also includes much more functionality that was not used in the Iranian train attack, he noted. It can: change passwords for all users; disable screensavers; terminate processes based on a list of target processes; install a screenlocker; disable recovery mode; changesboot policy error handling; create scheduled tasks; and log off local sessions, among other actions.

The fact that it has such broad capabilities seems to suggest that Meteor is not merely a one-off, but that its creators intend for it to be used in other attacks, Guerrero-Saade noted.

MeteorExpress attackers also dropped a standalone screenlocker, mssetup.exe,that blocks user input before creating a window that fills the entire screen before disabling the cursor and locking the user out entirely, according to the report.

Novice Attackers?

Despite its success in the MeteorExpress attack, the threat group seems still to be honing their skills and finding their way, as evidenced by the "contradictory" practices of Meteor's code and capabilities, researchers observed.

"First, the code is rife with sanity checks, error checking, and redundancy in accomplishing its goals," Guerrero-Saade wrote. "However, the operators clearly made a major mistake in compiling a binary with a wealth of debug strings meant for internal testing."

The guts of Meteor also include a "bizarre amalgam of custom code" that leverages open-source components and "practically ancient" software–FSProLabs' Lock My PC 4, pointing to the general experimental nature of the attackers' approach, he said.

However, "while that might suggest that the Meteor wiper was built to be disposable, or meant for a single operation," this code is "juxtaposed with an externally configurable design that allows efficient reuse for different operations," Guerrero-Saade wrote.

Overall, the components of MeteorExpress that researchers examined point to a new, intermediate-level player in the attack landscape "whose different operational components sharply oscillate from clunky and rudimentary to slick and well-developed," he concluded.

Source: https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/

12. Amazon gets $888 million GDPR fine for behavioral advertising

Amazon has quietly been hit with a record-breaking €746 million fine for alleged GDPR violations regarding how it performs targeted behavioral advertising.

The fine was issued by Luxembourg's Commission nationale pour la protection des données (CNPD), an independent public agency established to monitor the legality of the collection and use of personal information.

In an SEC Form 10-Q filed today, Amazon states that this massive fine came out of CNPD in July 2021, which fined them for improper processing of personal data.

"On July 16, 2021, the Luxembourg National Commission for Data Protection (the "CNPD") issued a decision against Amazon Europe Core S.à r.l. claiming that Amazon's processing of personal data did not comply with the EU General Data Protection Regulation," reads an SEC 10-Q filing submitted by Amazon today.

"The decision imposes a fine of €746 million and corresponding practice revisions. We believe the CNPD's decision to be without merit and intend to defend ourselves vigorously in this matter."

The decision comes from a complaint filed by La Quadrature du Net in 2018 against Amazon Europe Core SARL, Amazon EU SARL, Amazon Services Europe SARL and Amazon Media EU SARL, and Amazon Video Limited.

The complaint alleges that Amazon is analyzing users' behavior to build profiles used for targeted advertising. This creation of these behavioral profiles is being done without a user's consent and thus violates GDPR.

Amazon has told BleepingComputer that this fine is not related to a data breach or unauthorized access to customer data but rather how they perform advertising.

Amazon further states that they believe the decision is based on subjective and untested interpretations of the GDPR privacy law.

"We strongly disagree with the CNPD's ruling, and we intend to appeal," Amazon said in a statement to BleepingComputer.

"The decision relating to how we show customers relevant advertising relies on subjective and untested interpretations of European privacy law, and the proposed fine is entirely out of proportion with even that interpretation."

This fine is the largest ever issued by the European Union for GDPR violations. Before this decision, the largest fine was €50 million ($56.6 million at the time) against Google for not correctly receiving consent when processing user's data when creating a Google account or performing advertising.

Source: https://www.bleepingcomputer.com/news/technology/amazon-gets-888-million-gdpr-fine-for-behavioral-advertising/

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.sales@tbs.tech**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.