

Security Matters

Focus on Cyber Espionage

Cyber Espionage? We can hear you thinking, “this has nothing to do with me!” After all, we are just ordinary people who get up each day to lead ordinary lives where we stay in touch with family and friends on Facebook, send and receive email, shop a bit online, login to check our bank accounts, pay our bills, and share photos from our mobile phones. Nearly everyone uses a computer for doing their job, but most of us working for governments here in Montana don’t access systems that seem to be all that attractive to a cyber spy. The term “cyber espionage” often conjures up thoughts of spies from foreign countries trying to steal government military secrets, but that’s not the only use of cyber espionage.

The people behind cyber espionage have a variety of reasons

and objectives for their attacks. Three main ones are profit, power, and protest. Cyber criminals may hope to gain access to sensitive information in order to sell it to others or they may want to



use it themselves. Internal use is especially likely with industrial secrets or proprietary information. Information obtained may also provide criminals with the opportunity for profit through blackmail. Consider both the Ashley Madison and Sony

Device Hardening Strategy

The Montana Information Security Advisory Council (MT-ISAC) approved the Device Hardening Strategy at the February 2016 meeting. This document was researched and developed by the Best Practices workgroup. The goal of this strategy was to provide recommendations with no additional cost and low effort to increase the security of end-user workstations. The MT-ISAC Tools Workgroup will be developing recommendations for implementation.

Key points in the document in-

clude workstation configuration, patch management, limited administrative privileges, deployment of the Microsoft Enhanced Mitigation Experience Toolkit (EMET), Applocker use, elimination of mapped drives, device drive encryption, and SmartScreen Filter use.

For workstation configuration, the group recommends configuring all workstations with a fresh installation of the system’s operating system. The “Gold Image” should be validated against security benchmarks and should be updated

breaches where the perpetrators first asked for payment in return for not divulging the data they had acquired.

Note that cyber espionage is different from cyber criminals using ransomware to make money. Unlike cyber espionage attacks, ransomware doesn’t care what the files contain. The threat is to lock the files and threaten to destroy them unless a ransom is paid. The cyber criminal carrying out espionage is looking for sensitive information that can be used for profit due to its confidential nature. Cyber espionage depends on the availability of the data. Ransomware depends on the threat of destruction—or future unavailability of the data.

Blackmail may also play into the [Continued on page 5](#)

ed monthly to incorporate security updates.

Agencies should develop, implement, and audit compliance with a patch management policy and process for workstations.

Standard end-users should not have administrative privileges on their workstations due to the security risks which accompany those privileges.

EMET is a free tool for the use by systems administrators to enhance workstation security.

[Continued on page 3](#)

Security Matters is the monthly information security newsletter published by the Enterprise Security Program. Each month we also have a supplemental file of materials you can use for security awareness. You can find that file at: <http://sitsd.mt.gov/Montana-Information-Security/Security-Training-Resources>

We hope you’ll find the newsletter and materials useful and hope you’ll give us feedback on what we can do better. Your suggestions for topics and content are welcome. [Contact us.](#)

Inside this issue:

Current Threats & Vulnerabilities	2
Security Event Calendar	2
National Consumer Protection Week	2
MT Information Security Advisory Council	3
Security Training News	4
Training Resources	4
Awareness Event Prize Winners	4
News You Can Use	6



A monthly update on the latest security threats and other software news.

Sean Rivera, CISSP

Samsung TVs are Soooo 1984

In a review of the privacy statement published with Samsung’s SmartTV, there is one sentence that may make users feel like someone is always listening.

“Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party,” states the privacy policy.

Samsung SmartTVs, if con-

nected to an internet connection, allow for its users to embrace voice commands. However, as a result of that, the television’s microphone is perpetually on and listening for a directed command. If you use a SmartTV and have this feature enabled, be mindful of what you say around it. Samsung confirms that it does not retain or sell any of the data collected via the voice-command feature.

Ransomware Goes Hollywood....Sort Of

Due to an unfortunate circumstance, Hollywood Presbyterian

Medical Center experienced a difficult bout of ransomware that affected multiple critical systems. Due to the unspecified crypto-virus, the hospital was forced to turn away many emergency cases, and of those admitted during this time were done so using the old fashion method of paper and pen. Even nurse’s charting was done on paper forms. In order to restore continuity to its business, HPMC eventually paid nearly \$17k in ransom for the decryption keys.



National Consumer Protection Week 2016 takes place March 6-12. Go to <https://www.ncpw.gov> or <https://dojmt.gov/consumer/> to find consumer tips and free materials from government and private organizations. Be an informed consumer; avoid scams and fraud!

The Montana Department of Justice says,

In Montana, it’s illegal to rip people off. It’s illegal to lie about something you’re selling. It’s illegal for a business to be deceptive or unfair. These laws regulating commerce are a powerful ally for Montana’s consumers and business owners. They level the playing field and help us to protect our state’s consumers from those who would take advantage of them.

But the office does much more than that. We also track scams and alert citizens. We educate young people about buying their first car and renting their first apartment. We teach Montanans how to manage their credit reports and keep their personal financial information secret and safe. We reach out to farmers and ranchers — Montana’s first small businesses — and help them navigate a market that is increasingly controlled by a handful of large corporations.

*In today’s world, we all live in a global marketplace. If you need help finding your way around it or you feel you’ve been victimized, we are here to help. **Talk to your family. Talk to your friends. Talk to us.***

Security Awareness 2016 Events

Meet Us At META

- ◆ The Enterprise Security Program will have a booth at the Montana Educational Technologists Association Annual Conference—March 15-16, 2016 at the Helena Great Northern Hotel.

Focus on Email

- ◆ April 14, 2016 - 1:30—3:30 at OPI Training Room
1227 11th Ave



Check [Montana Information Security](#) for the latest event schedule and contact [Lisa Vasa](#) if you’d like to host an

Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting



February 18, 2016

Meeting highlights

OPI Security Plan

Curt Norman the Network Systems Analyst for the Office of Public Instruction gave a presentation OPI's Security Plan. This high level plan was developed for staff to give them an understanding of the importance of security and how OPI complies with federal standards and State of Montana statues and policies. This plan also serves as a roadmap for the agency on how security will be implemented throughout OPI's environment and systems.

Cybersecurity National Action Plan

Lynne Pizzini reviewed key points of President Obama's [Cybersecu-](#)

[rity National Action Plan](#) (CNAP) and encouraged everyone to review the National Action Plan. The plan includes establishing a Commission on Enhancing National Cybersecurity, made up of top strategic, business and technical thinkers from outside of Government. A new position will be created, Federal Chief Information Security Officer to drive cybersecurity changes across the Government. Fiscal year 2017 Budget includes over \$19 billion for cybersecurity which results to a 35 percent increase from FY 2016.

Council Approvals

Council approved the assessment workgroups suggestions for the Governors Dashboard with the addition of including information from the previous months Information Security Incident Reports.

Council approved the Device Hardening Strategy contingent on if IRS schism requirements are met during the harden workstation configurations process. UPDATE - The IRS schisms are met within the document by "validating against security benchmarks from trusted sources" in which one of those trusted sources can be IRS schisms.

Council approved to start the "Tools" workgroup for implementing the newly approved Device Hardening Strategy. Dawn Temple from Department of Justice will chair this workgroup. No date has been set for the first meeting, but anyone can contact Dawn Temple or Joe Frohlich if they would like to join this workgroup. Suggested members for this workgroup would be technical staff members who would

help decided on the best ways to implement Device Hardening Strategy.

Best Practices Workgroup

The Best Practices workgroup has identified a list of best practices based from the Information Security Policy. The MT-ISAC has been requested to review this list and help prioritize which best practices are worked on first.

desk to State agencies, cities, and counties. More threats were blocked in 2015 than any prior year.

Next Meeting

The next meeting will be **Thursday**, March 17, 2016 at 1:00 p.m. at the DEQ Lee Metcalf Building, Room 111. **Please note that the meeting has changed from the third Wednesday of the month to the third Thursday.**



Device Hardening from Page 1

Applocker is an application control and whitelisting feature in Windows 7 and Windows Server 2008 R2 that allows one to specify which users or groups can run particular applications based on unique identities of files. This provides administrators to control the types of applications, scripts, Windows Installer files, and DLL files. This helps to prevent users from running inappropriate applications. Applocker also provides

application whitelisting.

The elimination of mapped drives may not be possible for all agencies, but agencies should consider this if business processes allow for it. Malware, specifically ransomware, may target not only the local drive, but mapped network drives or devices, allowing the malware to spread. Elimination of mapped drives limits the extent of damage.

MT-ISAC also recommends using Bitlocker or other full-disk encryption of device drives. It is designed

to protect data in the event of physical loss of the device.

The final recommendation is to enable SmartScreen Filter in Internet Explorer. This feature helps detect phishing websites and helps to protect the user from downloading or installing malware.

For more information about the Device Hardening Strategy, visit the MT-ISAC website <http://sitsd.mt.gov/Governance/ISAC> or contact the [Enterprise Security Program](#).

[Focus continued from page 1](#)

the power motivation. It does not always have to do with money. Knowing secrets can provide a powerful tool for controlling individuals who wish to keep those secrets from being exposed.

The power motivation is also behind attacks that seek to disrupt activity or destroy assets. For example, recently a part of the Ukrainian national power grid was taken down by hackers resulting in a black out for more than 225,000 customers. The attack rendered the systems inoperable by destroying vital files as well as disrupting the management program for the “uninterruptible power supplies” which hindered efforts to restore electricity.

As the Internet of Things (IoT) becomes more and more pervasive, sabotage of the computers that control our things is also becoming a larger concern. We might not think of a hacker’s attack on a vehicle’s computer as a sign that the hacker is seeking power, but the underlying motive often is about having power over a person or a thing whether that power is for monetary gain or not.

You’ve may have heard the term “hactivist” at some point. A hactivist is a activist who uses hacking to promote his or her cause. The hactivist illustrates the third motivation for cyber espionage: protest. According to cyber security consultant Mandiant, attacks from hactivists greatly increased in 2015 and the trend is expected to continue. Some examples include defacing websites of companies and government entities, obtaining and sharing publically lists of management’s or law enforcement officers’ personal information (also called “doxing”) , or disrupting or destroying systems as a protest against policies or activities

Government, military, and private industries are all targets and while we may think our roles are insignificant when it comes to providing information or money, each of us is the target—the way into the organization. Attacks use familiar methods like distributed denial of service (DDoS) attacks, phishing, social engineering, malware on websites, and infected USB drives. They leverage unpatched

systems and zero-day vulnerabilities. What generally sets cyber espionage apart from the usual malicious attacks is the planning and organization behind focused attacks on specific targets.

So what do we do? From an organizational standpoint, it’s important to implement security controls including (but not limited to) patch management, configuration management, incident response, limited administrative privileges, and access controls. But each of us as individuals also have a role in protecting the information to which we have access. Recognizing that even our personal information is valuable to cyber criminals means we need to be as vigilant at home as we are at work.

We can each take steps toward preventing cyber espionage by practicing good security habits:

- Start with strong, unique passwords for all the systems and devices to which you have access. Change your passwords regularly and never share them with anyone. If you are the administrator for applications, databases, or devices at work, make sure that the admin password is not the default password installed with the system. Change it regularly, too.
- Keep all your applications, web browsers, and devices updated and patched. If you are responsible for systems at work, this is especially critical.
- Think before you click on a link. We can’t stress this enough! Phishing is increasingly difficult to recognize. Take the extra minute to closely examine emails you receive which contain links.
- Watch for social engineering attempts. Don’t let your desire to help someone get in the way of following policies and procedures. Always verify requests for sensitive information or access into restricted areas. And remember—if it sounds too good to be true, it probably is.

- Use strong passwords or passcodes for your mobile devices and use encryption when possible. Report lost or stolen devices immediately.
- When working in public areas, make sure that your screen is not visible to others in the area. Use secure networks or a VPN when connecting to the internet.
- Limit the information you share on all social media accounts. Review the privacy settings on the accounts periodically as they may have changed. Don’t use information available online about you as your passwords or passcodes. Information you share can also cyber criminals to create fake accounts or impersonate you to obtain passwords or access.
- Don’t fall for baiting attacks like USB drives left in public areas for you to “find”. Only connect approved devices to the network.
- Use antivirus or anti-malware software. Keep the software up to date and configure it to run automatically. If your device becomes infected, report it immediately to your IT staff. At home, make sure you are also protected and if infected, consider hiring a reputable professional to clean your device.

Cyber espionage may conjure up visions of the hackers and spies targeting military or industrial secrets, but it is increasingly common in our connected world. Do your part to protect yourself and your organization



News You Can Use

[US Government Confirms Cyber Attack Against Ukrainian Critical Infrastructure](#)

Investigators have officially confirmed that the devastating power outages experienced in the Ukraine last December were the result of a cyber attack.

[Does Connecting Your Phone To Your Car Open Up New Security Risks?](#)

'Always on' nature of today's software-reliant cars means using your smartphone on the road opens up additional attack vectors and vulnerabilities.

[It's Tax Season, and States Are Battling Bogus Requests for Refunds](#)

Tax fraud costs state treasuries millions of dollars. This tax season, states are employing new strategies to combat online tax fraud.



OMG! STOP RIGHT MEOW!
TINY SECURITY CAT
IS NOT LETTING YOU DOWNLOAD
THAT SOFTWARE UNTIL
YOU CHECK COMPANY POLICY

SAC the security awareness
COMPANY
© 2014 THE SECURITY AWARENESS COMPANY

Security Quick Tip

Don't login to untrusted computers. Your password is only as secure as the computer or network on which it is used. Don't use public computers to do banking, shopping, or accessing work.

For more security tips, news, advisories, and resources visit the Montana Information Security website, find us on Facebook, or follow us on Twitter.

<http://sitsd.mt.gov/MontanaInformationSecurity>

 State of Montana Information Security

 @MontanaSecurity

Contact Us:

[Enterprise Security Program](#)

[Lynne Pizzini, CISO and Deputy Chief Information Officer](#)

[Joe Frohlich, Enterprise Security Manager](#)