Анализ атаки Petya.A Ransomware и некоторые рекомендации по совершенствованию защиты от Microsoft

По результатам анализа кибератаки с использованием вируса Ransom:Win32/Petya рекомендуется использовать такие процедурные и технические рекомендации для решения срочных, ближайших и перспективных задач.

Дополнительно, настоятельно рекомендуется заказать плановые сервисы Microsoft, которые призваны внедрить комплексные решения и рекомендованные практики:

Во вложении Вы также найдете презентацию с описанием развития атаки Ransom:Win32/Petya в большинстве организаций и компаний.

Действия, которые необходимо выполнить незамедлительно, **в случае заражения**. Целью данных мероприятий является остановка распространения вируса:

- Use special admin accounts for every subset of administration tasks; Use delegation of administrative tasks to support desk accounts with restricted right – Shares Cleanup
- Reset all Active Directory User Passwords, including Service Accounts, and then Krbtgt account reset after advise of Microsoft Support
- Search for Infected machines: look through Antivirus logs, Network Logs (example look for machines scanning for tcp/139 and tcp/445 services) – look for infection files … (https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/)
- Isolate and cleanup infected workstations/servers by running, for example, boot usb/iso disk with Microsoft Offline Defender (https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc),

  Microsoft Security Essentials Windows 7(https://support.microsoft.com/en-us/help/14210/security-essentials-download), Windows Defender Windows 8,Windows RT, Windows 8.1, Windows RT 8.1, Windows 10.

  Microsoft Antimalware detects Petya (known variants) starting definition version **1.247.197.0**

- Block or restrict access to specific IPs for file-sharing services (SMB)

  netsh firewall set service fileandprint

  netsh firewall set service RemoteAdmin disable

- While you assess the impact and apply definition updates.
  - Block any traffic on ports 139 and 445 to prevent propagation either into or out of machines in the network.
  - Disable remote WMI and file sharing.

These may have large impacts on the capability of your network, but may be suggested for a very short time period

- Cleanup and remove as much as possible the accounts with Local Administrators rights on workstations/servers you have got Local Access

- Use App Locker or Software Restriction Policies in Group Policy to block execution of certain programs (e.g. PSEXEC) or unsigned binaries (e.g. Petya's DLL library) for machines that cannot benefit from Device Guard due to lack of the specific hardware requirements or due to older operating systems not supporting new mitigations (e.g. Windows 7).

Далее выполнить такие контрольные проверки рабочих станций/ссерверов и объектов в ИТ-среде

- Securing Privileged Access https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access
- Additional Accounts restrictions practice:
    - Enforce different password used for users and administrators accounts
    - Delete Users member of the administrators group
    - Delete service account member of administrators group
    - Block domain administrators connecting remotely on workstations
    - Passwords with 14 or more symbols
- Email hygiene - stop your users from getting phished - block what you can, user do not need exe and every other flavor of executable to be sent via email.
  "For increased protection, we also recommend using Transport rules to block some or all of the following extensions: ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh. This can be done by using the **Any attachment file extension includes these words** condition."
- Turn on SmartScreen to filter the web links
  If your running current OS turn on Device Guard protections in windows 10
  If you are running O365 make sure you have enabled ATP
  If you can disable SMB v1 great - plats can help - it does break some backwards compatibility. Next is turn of file shares and limit rights to read only where they can. if Ransomware can modify it does.
- Use UEFI Secure Boot as the security standard to boot workstations/servers/ This is use hardware features to protect boot process and firmware against tampering.
- You need to be current on at least the security only updates - run either WU or MBSA to verify unless you have another management solution

  Specifically, for this issue, ensure Microsoft Security Bulletin MS17-010 Security Update for Microsoft Windows SMB Server is installed. This is the link to the most recent - https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99 being the June 2017 Security Updates.
- Keep the Anti-malware signature is up-to-date. Windows Defender, System Center Endpoint Protection, and Forefront Endpoint Protection detect this threat family as Ransom:Win32/WannaCrypt.

In addition, the free Microsoft Safety Scanner http://www.microsoft.com/security/scanner/ is designed to detect this threat as well as many others.

- Make sure that users have the level of knowledge required to never click on suspicious attachments even if they are displayed with a familiar icon (office or PDF document). Where an attachment opening offers the execution of an application, users must under no circumstances accept execution and in doubt, users should you consult and/or consult the competent computer.

Malware response procedure is described here at link and attached to email https://technet.microsoft.com/en-us/library/cc162838.aspx

- Review the Microsoft Security Response Center (MSRC) blog at Customer Guidance for WannaCrypt - Attacks for an overview of the issue, details of the malware, suggested actions, and links to additional resources.
- Customers who believe they are affected can contact Customer Service and Support by using any method found at this location: https://support.microsoft.com/gp/contactus81?Audience=Commercial.
- If you feel you have detected a new threat, sample, can you retrieve a sample of the malware and send it to the Microsoft Malware Protection Team? https://www.microsoft.com/en-us/security/portal/submission/submit.aspx

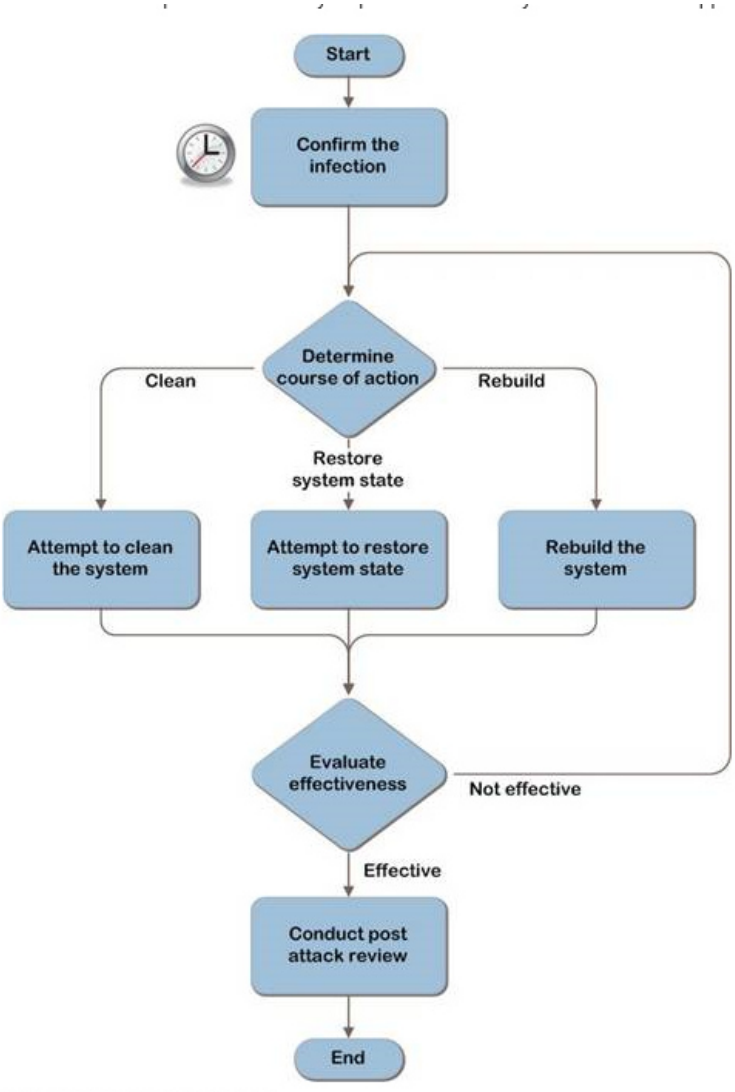

Figure 1. Decision flow chart

В дальнейшей перспективе для систем Windows XP (следует вывести из эксплуатации в кратчайшие сроки!), Windows 7/8 использовать **E**nhanced **M**itigation **E**xperience **T**oolkit https://technet.microsoft.com/en-us/security/jj653751, анализатор поведения пользовательских учетных записей Microsoft ATA (https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics) в сети Active Directory, а также Microsoft Advanced Threat Protection, использовать встроенный в операционную систему Windows Defender Antivirus, и бесплатно загружаемый Microsoft Safety Scanner http://www.microsoft.com/security/scanner/, в случае использования сервисов Office 365 также оценить возможность использования Office 365 Advanced Threat Protection, Multifactor Authentication.

Рассмотреть возможность использования по три разные системы защиты на каждое потенциальное направление кибератаки.

Прошу обратить Ваше внимание, что комплексный характер атаки позволяет говорить о сохраняющемся высоком риске повторного заражения.

Для снижения данного риска рекомендуется выполнить следующие мероприятия, в том числе по обучению Вашей ИТ-командам навыкам решения проблем в условиях кризиса безопасности и во время восстановления после атаки или компрометации ИТ-системы, с привлечением Microsoft Consulting Services и Premier Support или в удаленном режиме, или у Вас на площадке:

Actions	**Microsoft Technology**	**Microsoft Services Solutions**
1	**2**	**3**
Immediate & Short Term Actions plan! 2-3 weeks		
Ad – Cleanup and review Separate Admin account for admin tasks – Delegation – Shares	Microsoft Security Advisor	Consulting Microsoft
Reset All active Directory User Passwords	Microsoft Security Advisor	Consulting Microsoft
Privileged Access Workstations (PAWs) ***Phase 1 - Active Directory admins***	Windows 10 Enterprise	Privileged Account Workstation (PAW) Enhanced Security Administrative Environment (ESAE)
Unique Local Admin Passwords for Workstations	Local Administrator Password Solution (LAPS) http://aka.ms/LAPS	Securing Lateral Account Movement (SLAM) Lateral Traversal Mitigation (in pilot)
Unique Local Admin Passwords for Servers		
Offline AD Security Assessment	ADS – Active Directory Security Assessment	Microsoft Premier
Mid-Term Actions plan		
Securing Windows Active Directory Workshop		Microsoft Premier

1	2	3
Attack Detection	ATA Implementation Services (ATAIS) Strongly recommended services solution to enable customer to handle events!	Advanced Threat Analytics (ATA) http://aka.ms/ata
Build a Long Term Security Strategy based on result on Offline AD Security Assessment	MSRA Offering – Microsoft Security Risk Assessment	Consulting Microsoft

Выполнить оценку текущего состояния процессов и технологий обеспечения безопасности, чтобы подготовить стратегию обеспечения безопасности и плана по ее реализации, рекомендуется в рамках сервиса Microsoft Security Risk Assessment

Для выполнения задач администрирования рекомендуется внедрять выделенные защищенные станции администрирования Privileged Access Workstations

https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/privileged-access-workstations

Для назначения временных прав и ведения полного аудита выполнения работ по сопровождению ИТ-систем учетными записями с повышенными привилегиями предназначено решение Privileged Access Management for Active Directory Domain Services и основано на использовании Microsoft Identity Manager

https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Рассмотреть возможность использования по три разные системы защиты на каждое потенциальное направление кибератаки.

Дополнительно выполнять мониторинг бюллетеней безопасности и обновления рекомендованных практик на

- Microsoft Malware Protection Center (MMPC) post #2: Windows 10 platform resilience against Petya
- Microsoft TechCenter: Security Resources to Help Disrupt Lateral Movement
- The new Microsoft Malware Protection Center blog: https://blogs.technet.microsoft.com/mmpc