

Measures for response and prevention of Targeted Attacks (Advanced Persistent Threats)

If any system is suspected to be infected or any email account is subjected to unauthorised access the following measures shall be considered.

I. Incident Response Measures:

1. Determine accounts accessed by foreign IPs and unauthorised IPs.
2. Determine computers/laptops and mobile devices used to access such affected email accounts ✓
3. Isolate the same from network. Take forensic image of the same and preserve for further analysis. Collect volatile evidence like memory dump also. ✓
4. Preserve all the logs of the network where affected systems are located and analyse the same ✓
5. Collect email access logs of affected email account and determine unauthorised access (IPs).
- ✓ 6. Take backup of important data and clean the suspected affected systems with latest anti virus. Preferably the antivirus software to be installed on a bootable CD/ Pendrive and infected system should be booted through such alternate drive.
7. Share forensic image of the affected system alongwith analysis report and actions taken at organisational end with CERT-In for further analysis.

II. Incident Prevention Measures:

- Block / Restrict connectivity to the malicious domains /IPS shared by CERT-In from time to time. If any of the machines found contacting them, take volatile evidence, isolate the machine, start necessary mitigation and containment procedures. Take forensics image of the machine for root-cause analysis. It is recommended that, restore the system from a known good back up or proceed to a fresh installation.
- Keep up-to-date patches and fixes on the operating system and application software such as client side software's, including Adobe Products (reader, flash players), Microsoft Office suites, browsers & JAVA applications. Refer **Appendix A**
- Restrict execution of powershell /WSCRIPT in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis. Reference:https://www.fireeye.com/blog/threatresearch/2016/02/greater_visibility_t.html

- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
- Control outbound DNS access. Permit internal enterprise systems to only initiate requests to, and receive responses from, approved enterprise DNS caching name servers. Monitor DNS activity for potential indications of tunnelling and data exfiltration, including reviewing DNS traffic for anomalies in query request frequency and domain length, and activity to suspicious DNS servers. The dnscat2 tool alternates between CNAME, TXT, and MX records when it is operating. Investigate abnormal amounts of these records going to the same second level domain, or a group of second level domains.
Reference: <https://www.us-cert.gov/ncas/alerts/TA15-240A>
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf>
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Deploy Microsoft's Enhanced mitigation Experienced Toolkit (EMET) which provides end node protection against zero day vulnerabilities and blocks and prevents memory based attack approaches.
<http://support.microsoft.com/kb/2458544>
Detailed steps for EMET configuration are described in **Appendix B**.
- Enhance the Microsoft Office security by disabling ActiveX controls, Macros, Enabling Protect View, File Protection Settings. Steps for configurations are mentioned in **Appendix-C**
- Apply software Restriction policies appropriately. Disable running executables from unconventional paths. Steps for configurations are detailed in **Appendix-D**
- Protect against drive-by-downloads through controls such as Browser JS Guard and Sandboxie (**Refer Appendix-E**)
- Leverage Pretty Good Privacy in mail communications. Additionally, advise the users to encrypt / protect the sensitive documents stored in the internet facing machines to avoid potential leakage
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header). Block the attachments of file types,
"exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Enable a personal firewall on workstations.
- Disable unnecessary services on agency workstations and servers.
- Exercise caution when using removable media (e.g. USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

III. Measures for enhancing security of ICT infrastructure

- Define an appropriate network architecture including both the network perimeter, any internal networks, and links with other organisations such as service providers or partners. Manage the network perimeter by control access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content.
- Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Employ effective processes for managing changes to avoid workarounds.
- Network Intrusion detection / prevention and other appropriate security devices should be deployed and monitored by trained personnel. Alerts generated from the devices should be thoroughly verified as most of them could be an imminent attack.
- Follow the best practices defined in ISO 27003 while designing and segregating network resources
- Execute Access to local operating system accounts with **system-level administrative** rights is **restricted** to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software

installation and configuration, maintenance, and emergency activities. At all other times, the Accounts are restricted from being accessed.

- System hardening applies the security concept of “least privilege” to a system by disabling features and services that are not required for normal system operations. This process reduces the system capabilities, features, and protocols that a malicious person may use during an attack. Attackers leverage genuine native utilities available in the Operating systems to lateral movements and to make persistence.
- Regular check on the configuration changes and appropriate usage of configuration and **change management**. In most cases, miscreants were successful in making changes to critical monitoring devices to exclude certain operations so as to hide their tracks. Stringent change management policies on Enterprise security devices such as Firewalls, AV gateways, Mail servers, DNS records, Active Directories and enforcing effective change control policies.
- Baseline the regular activities of end-point devices and servers. Diligently identify behaviours such as successful RDP connections/ SSH logins, new System Services/ processes, new installed applications/ software's, new User account Creations, command history, log in user history, network usages and changes in system configurations, disabled AV, System Services etc.
- The Critical servers are either made stand-alone or member of a dedicated secure zone Active Directory forest to use either local authentication or a secure zone dedicated authentication system (for example dedicated instance of LDAP/RADIUS solutions) to protect the secure zone against compromise of the enterprise central authentication systems including theft of authentication credentials to avoid pass-the-hash and pass-the-token attacks.
- Check for unnecessary connectivity towards Content Delivery Networks, as malware are known to tunnel the connection towards these domains to hide their traffic and towards DDNS / free top level domains. Examples **publicvm.com, linkpc.net, zzux.com, chickenkiller.com, crabdance.com, ignorelist.com, jumpingcrab.com, moo.com, strangled.net, twilightparadox.com etc.** Regular auditing of the failed connection attempts from DNS logs, proxy logs and to successful connection towards unknown domains. Some of the attacks use unconventional usage of DNS queries to exfiltrate/ interact with the attackers [DNS TXT Records]
- Deploy SysMon for windows systems. Microsoft SysInternals Tool SysMon, is able to monitor and log system activity to the Windows Event Log. It can provide information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event

Collection or SIEM agents, and subsequently analyzing them, Network Defenders and System

Administrators can identify malicious or anomalous activity and understand how intruders and malware operate on their networks.s

- POWERSHELL LOGGING AND BEST PRACTICES

We have observed that malicious powershell scripts successfully bypass security devices by leveraging obfuscation and performing code injection on the fly TO OTHER processes without dropping malicious code to disk, effectively granting arbitrary code execution. PowerShell is integrated with the .NET Framework and has full access to Component Object Model (COM) and Windows Management Instrumentation (WMI) functionality and WinAPI's

PowerShell can be run locally or across the network through a feature known as Windows Remote Management (WinRM). To facilitate the use of WinRM, remote workstations and servers on which code is executed must have remoting enabled. Microsoft Windows Server 2012 and newer Microsoft Windows operating systems have remoting enabled by default.

Organizations should install latest version [V0.5]where possible due to the superior logging capabilities provided over earlier versions[can consider disabling the previous versions]

- o Powershell Best practices

- PowerShell V.5 With Applocker And Device Guard
- Execution of signed PowerShell scripts only which ensures authenticity and integrity
- **Log Powershell activity and push to a centralised logging systems for strict monitoring particularly activities related to "BITS transfer, Scheduled Tasks, active directory, Group Policy, WinRM, Network /firewall, Server Manager ,SMB share. Search for specific key words such as Invoke-Mimikatz, Invoke-ReflectivePEInjection, System.Runtime.InteropServices.MarshalAsAttribute, Win32Functions.VirtualAllocEx.Invoke.**
- PowerShell Constrained language mode/ PSLockDownPolicy to restrict the usage of advanced features such as such as .NET and Windows API calls and COM access
<https://blogs.technet.microsoft.com/kfalde/2017/01/20/pslockdownpolicy-and-PowerShell-constrained-language-mode/>

- It is strongly advised that these options be thoroughly be tested before deployment. Legitimate scripts using these features may cease to function.

References

<https://blogs.technet.microsoft.com/psverschell/2016/08/09/powershell-the-blue-team/>

<https://docs.microsoft.com/en-us/windows/device-security/device-guard/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies>

- Device Guard on Windows 10 and Windows Server 2016 can be used to enforce constrained language mode and application whitelisting by leveraging advanced hardware features where supported.
<https://docs.microsoft.com/en-us/windows/device-security/device-guard/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies>
- Check for unrecognized tasks being registered in task scheduler using "Schtasks /Query /FO LIST /V"
Check for entries in BITS run "bitsadmin /list"
Check for unauthorised WMI instances being registered.
[<https://msdn.microsoft.com/en-us/library/ff647965.aspx>]
- Configure the following parameter in the registry on all PCs running Windows 7 (and up) and all the servers using Windows 2008R2, to prohibit storing unencrypted passwords in RAM (which are usually leveraged by Mimikatz)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential=0
- Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators. We recommend that you use only Logon type 2 (interactive): [https://technet.microsoft.com/en-ie/library/cc787567\(v=ws.10\).aspx](https://technet.microsoft.com/en-ie/library/cc787567(v=ws.10).aspx). Block RDP connections originating from untrusted external addresses unless an exception exists; routinely review exceptions on a regular basis for validity.
- Prohibit a standard local administrator with an ID=500 (which is vulnerable pass-the-hash attack). Add another administrator and install updates to protect against

Pass the hash attacks:

<https://technet.microsoft.com/en-us/library/2871997#ID0E3D>

- Enforce application whitelisting /Software Restriction Policies on all endpoint workstations. This will prevent malware droppers or unauthorized software from gaining execution on endpoints. Leverage Group Policy / Applocker to strict enforcing of applications running from %appdata%, %tmp%, %temp%, %localappdata%, %programdata%,
- Minimize and completely deny granting administrator privileges for users of local PCs, especially for users who work with external information systems.
- Use a different local Administrator account password on every node, which must not match any domain administration credentials. If this rule is not currently applied – change all the passwords, make them unique, long and complex. Securely manage local Administrator passwords by using specialized tools, such as Microsoft's Local Administrator Password Solution (LAPS).
- Isolate hosts in the same VLAN, so that one workstation would not be able to gain access to another one on network levels L2/L3, and could access shared network segments (printers, servers, etc.)
- Provide timely updates of OS, antivirus software and other applications.
- Configure the service accounts with the minimum set of permissions necessary for them to function properly (with respect to logon type and group membership). Strictly prohibit adding service accounts to the local administrators group unless absolutely necessary.
- Ensure the integrity of data, system and application software deployed on the infrastructure servers; introduce application whitelisting on workstations.
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

- Restrict the usage of USB devices in the sensitive zones, blocking access to physical ports/ whitelist the known devices.
- Deploy effective enterprise asset management strategies to keep track of software versions that are installed on all the devices.
- Perform regular red-team / blue team exercises on the network to re-establish the rules, configurations and policies.
- Conduct security audit as per the stipulated standards on regular basis. Services of CERT-In empanelled auditors may be availed. (refer Cyber security Assurance section on website of CERT-In <https://www.cert-in.org.in/>)
- Visit the website <https://www.cyberswachhtakendra.gov.in/> for alerts on malware threats, free bot removal tools and security best practices and resources.

Appendix A

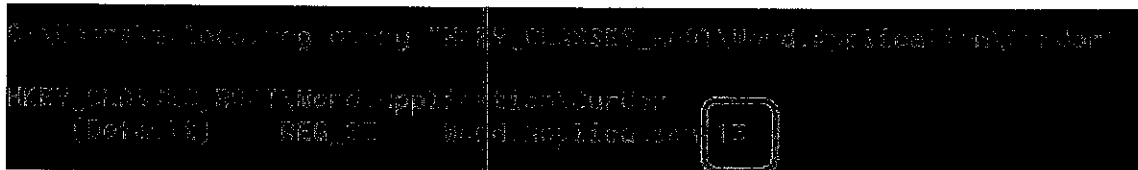
Update Microsoft Office software

- Turn on automatic updates appropriately for your OS.
- Manual update for OS /MS office.

Find the current version of the Microsoft Version

Open a command prompt and enter the command to find the office version stored from registry

reg query "HKEY_CLASSES_ROOT\Word.Application\CurVer"



```

C:\Users\laxmanp> reg query "HKEY_CLASSES_ROOT\Word.Application\CurVer"
HKEY_CLASSES_ROOT\Word.Application\CurVer
    (Data) REG_SZ Word.Application 15
  
```

Parse the output to get the version number and **match** against the list of existing Microsoft office versions to get the name of the version installed:

Version Number from registry	Version
15	Office 2013
14	Office 2010
12	Office 2007
11	Office 2003
10	Office XP
9	Office 2000
8	Office 98
7	Office 97

- For office 2013, choose File > Account > Update Options > Update Now of WORD menu.(applicable to all office applications)
- For office 2010, File > Help > Check for Updates.
- For 2007, select Microsoft Office Button > Word Options >Resources > Check for Updates.

Appendix B

Configuring EMET (Enhanced Mitigation Experience Toolkit)

EMET enables deploying and configuring security mitigation technologies that guard your PC from exploits by diverting, terminating, blocking, and invalidating those actions and techniques.

EMET can be downloaded from here.

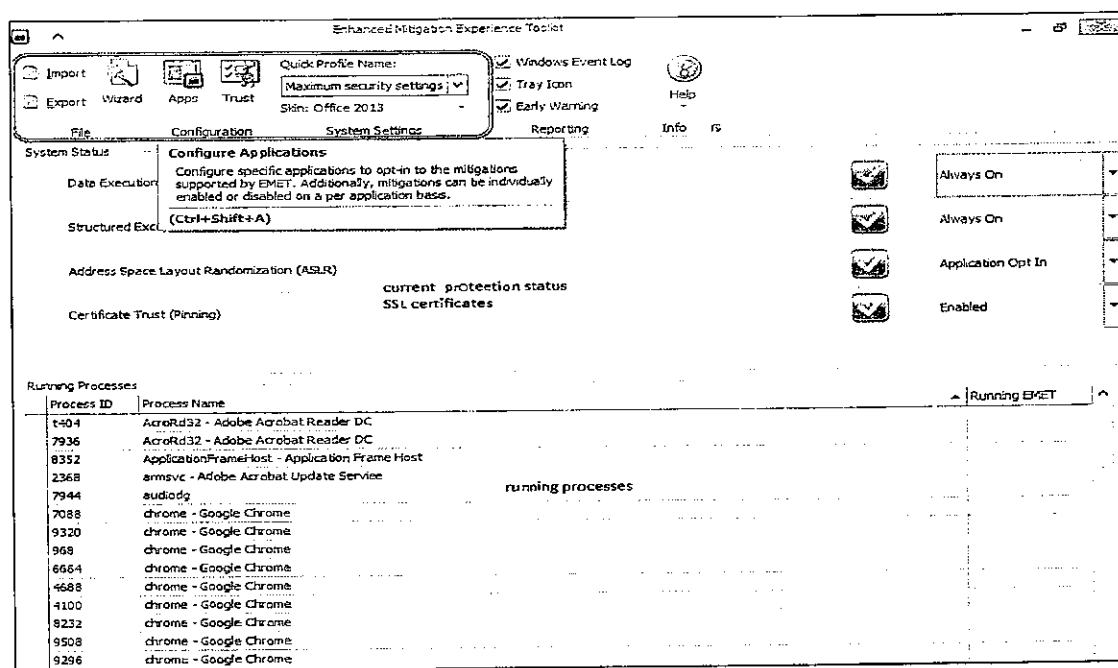
<http://www.microsoft.com/en-us/download/details.aspx?id=43714>

EMET forces applications to use several key mitigations built into Windows including Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Structured Exception Handler Overwrite Protection (SEHOP). DEP prevents data from executing and ASLR prevents malware from assembling its malicious activity from (multiple and specific) memory locations assigned in the system's memory. SEHOP prevents malware from overwriting entries in the structured event handler and malicious code referenced by that entry.

Details can be seen here:

<https://technet.microsoft.com/en-us/security/jj653751>

The basic and necessary configuration has been explained below:



First pane is categorised onto FILE, CONFIGURATION, SYSTEM SETTINGS, REPORTING, INFO sections.

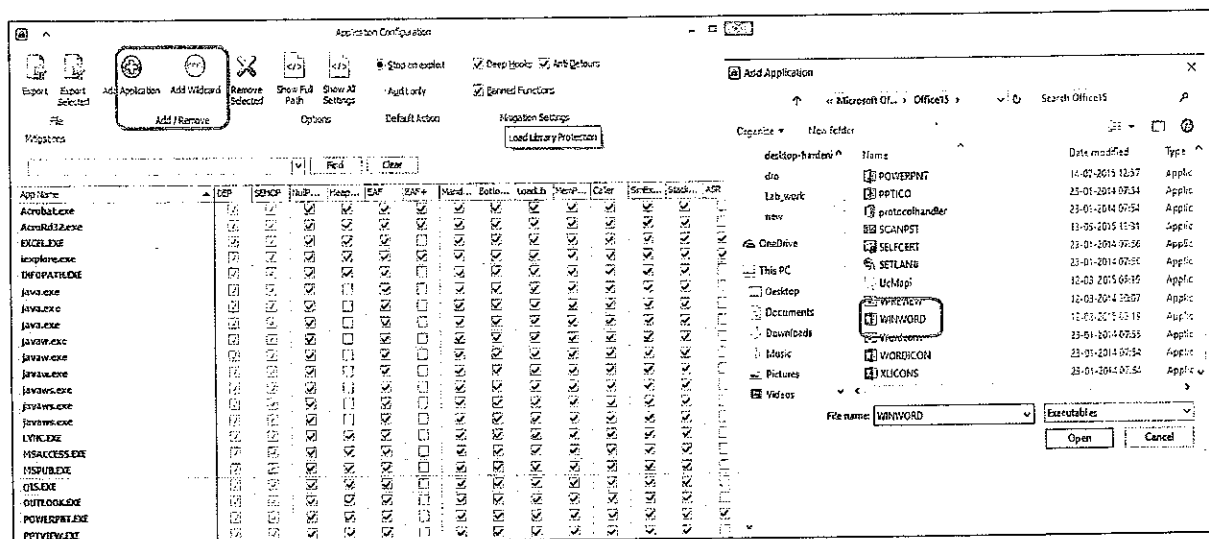
- File sections allows to "Import" (Ctrl+Shift+I) or "Export" (Ctrl+Shift+E)
- Configuration: access the "Application Configuration" window by clicking on "Apps" (Ctrl+Shift+A), and the "Certificate Trust Configuration" window by clicking on

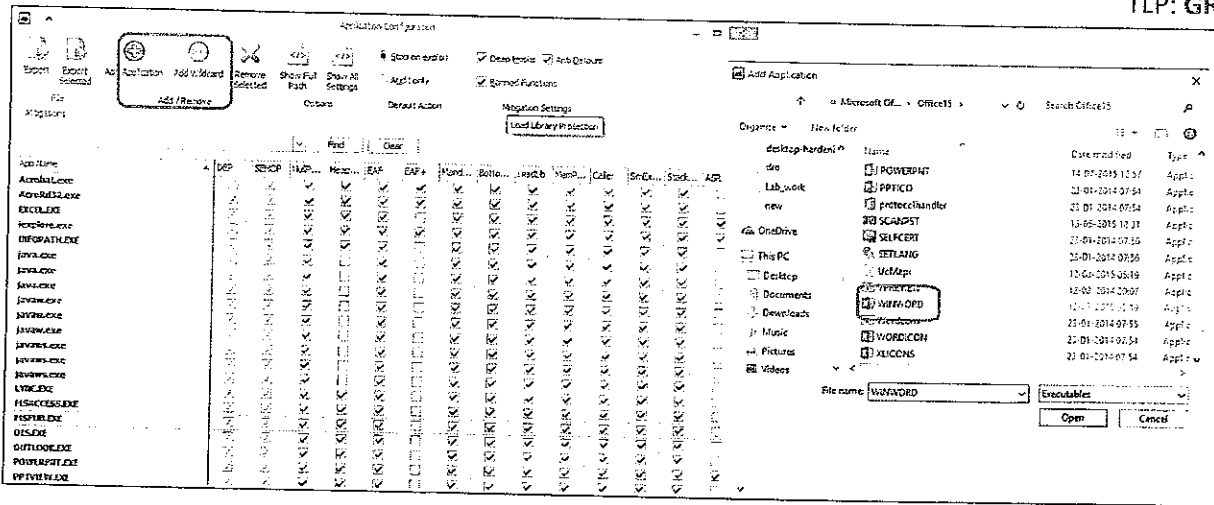
"Trust" (Ctrl+Shift+T). The certificate pinning is a recent feature introduced, where in EMET adds additional checks during the certificate chain trust validation process, with the goal to detect man-in-the-middle attacks over an encrypted channel. Each time a certificate chain trust is built by Internet Explorer for a SSL certificate while browsing to an HTTPS website, EMET will validate the end-entity SSL certificate and the Root CA that issued that certificate against the corresponding pinning rule configured by the user.

- System Settings: apply a Quick Profile for the system, as well as select a Skin for EMET GUI
- Reporting: This group allows toggling the Reporting options. It is possible to configure the reporting of EMET alerts granularly. When EMET detects an exploitation attempt or a SSL certificate that violates one of the pinning rules, the EMET Service can be configured to perform one or more actions: writing to the Windows Event Log, display an alert to the user, and/or use the Early Warning Program
- Help: resources, such as the Support Forums, and the User Guide (Ctrl+Shift+F1), and to access to the EMET Privacy Statement.

The middle pain specifies the current mitigation techniques & ssl certificates status. The lower pain details the current running status of the processes and the details of the EMET protections enabled.

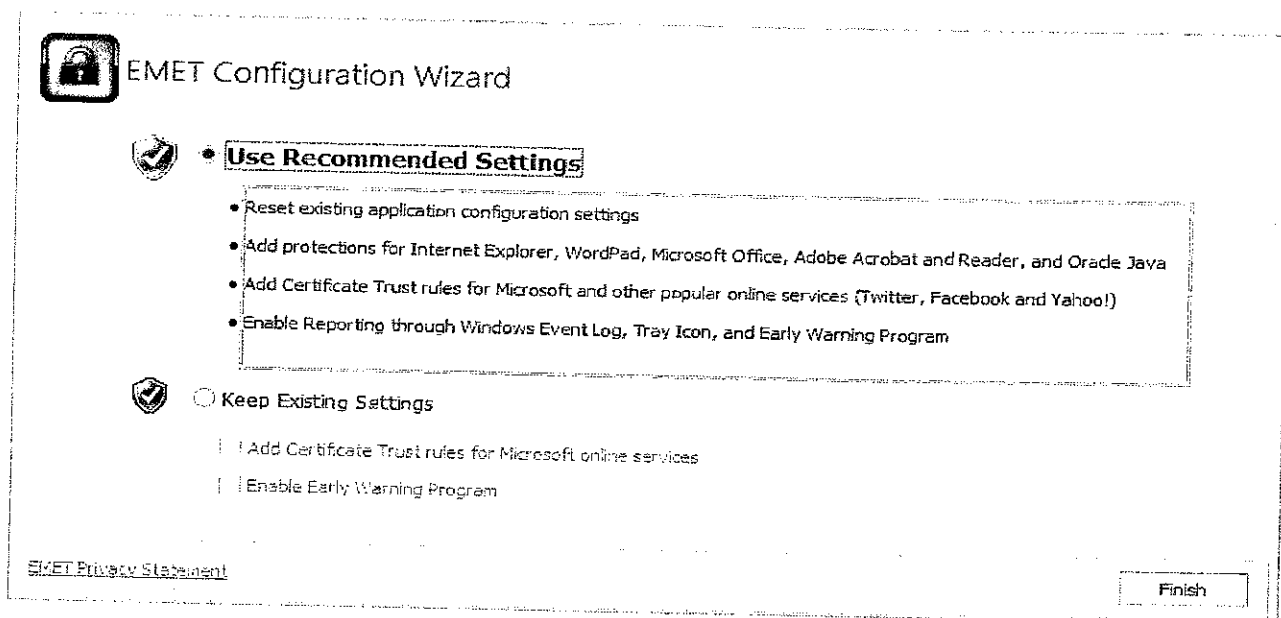
It is advised to enable these options on workstation, [DEP > always ON, SEHOP>always on, ASLR >Application Opt in, Certificate Pinning > Enabled]





The recommended settings of the configuration wizard, adds protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java. It also Configures EAF+ (Export Address table Access Filtering +) with Internet Explorer with the Microsoft Trident engine, the Adobe Flash plugin, the Microsoft VML plugin, the Microsoft VBScript engine, and the Microsoft JavaScript engine.

It configured to block the Adobe Flash plugin from running in Microsoft Excel, PowerPoint, and Word (largely seen in targeted attacks), and blocks the Oracle Java, Microsoft VML, Microsoft MSXML 4.0, Windows Script Host Runtime, and Microsoft Scripting Runtime plugins from running in Internet Explorer in websites not belonging to the Trusted Sites or Intranet zones.

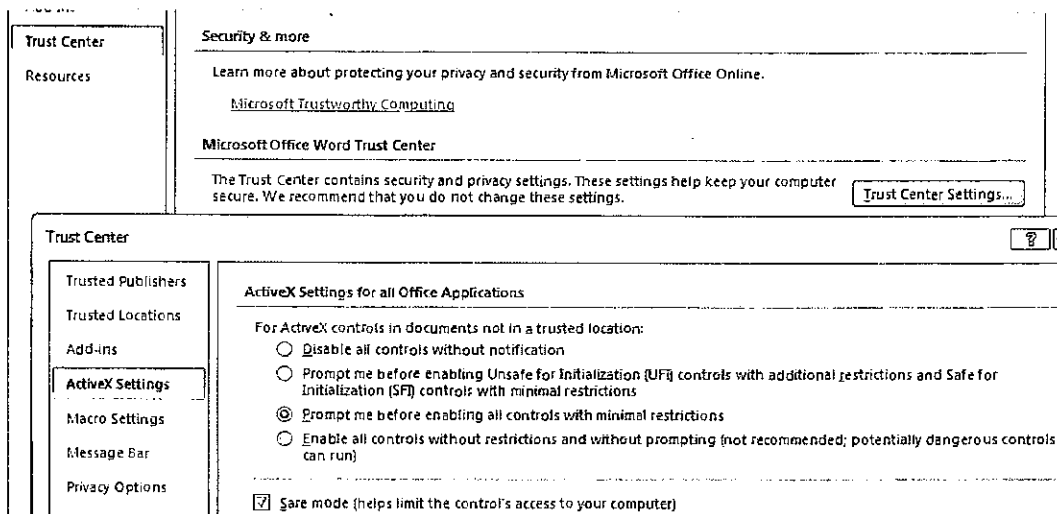


Appendix-C

MS OFFICE best Security Practices

1. Disable or prevent ActiveX controls in Microsoft Office Word Document from running without prompting.

Click **Office Button-> Word Options -> Trust center-> Trust Center Settings-> ActiveX Settings**

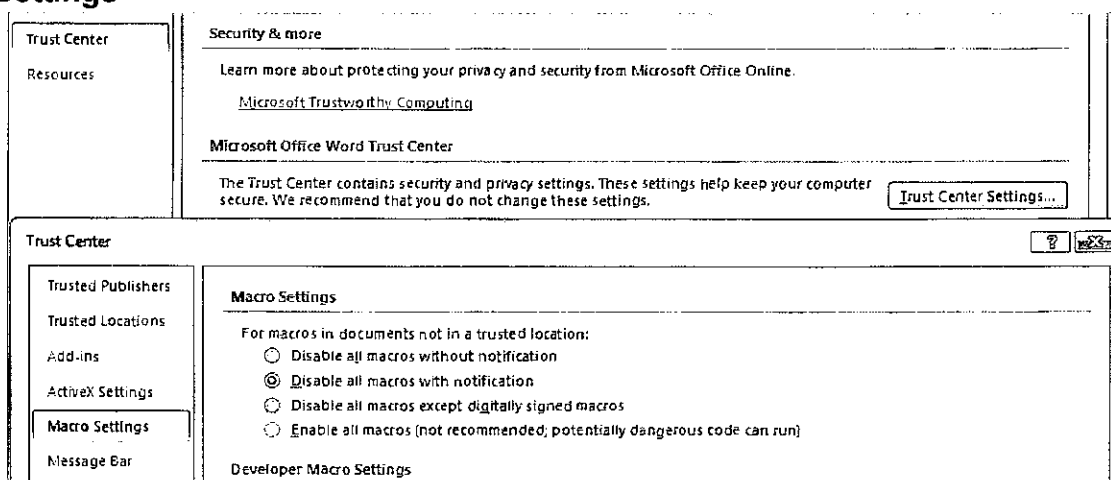


For more details, visit

<http://blogs.technet.com/b/srd/archive/2012/04/10/ms12-027-enhanced-protections-regarding-activex-controls-in-microsoft-office-documents.aspx>

2. Disable Macros in Microsoft Office Word documents.

Office Button-> Word Options -> Trust center-> Trust Center Settings-> Macro Settings



3. Configure built in "File Protection Setting" feature in Microsoft office 2010
Office Button-> Word Options -> Trust center-> Trust Center Settings->

File Type	Open	Save
Word 2007 and later Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
OpenDocument Text Files	<input type="checkbox"/>	<input type="checkbox"/>
Word 2007 and later Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 2003 Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 2003 and Plain XML Documents	<input type="checkbox"/>	<input type="checkbox"/>
Word XP Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 2000 Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 97 Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 95 Binary Documents and Templates	<input type="checkbox"/>	<input type="checkbox"/>
Word 6.0 Binary Documents and Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Word 2 and earlier Binary Documents and Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web Pages	<input type="checkbox"/>	<input type="checkbox"/>
RTF Files	<input type="checkbox"/>	<input type="checkbox"/>
Plain Text Files	<input type="checkbox"/>	<input type="checkbox"/>
Legacy Converters for Word	<input type="checkbox"/>	<input type="checkbox"/>
Office Open XML Converters for Word	<input type="checkbox"/>	<input type="checkbox"/>

Open behavior for selected file types:

☐ Do not open selected file types

☒ Open selected file types in Protected View

☐ Open selected file types in Protected View and allow editing

Restore Defaults

4. Configure built in feature for "Protected View" settings in Microsoft Office 2010 to open the Microsoft Office word documents in Protected view:
Office Button-> Word Options -> Trust center-> Trust Center Settings->Protected View

Microsoft Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

Trust Center Settings...

Protected View

Protected View opens potentially dangerous files, without any security prompts, in a restricted mode to help minimize harm to your computer. By disabling Protected View you could be exposing your computer to possible security threats.

☒ Enable Protected View for files originating from the Internet

☒ Enable Protected View for files located in potentially unsafe locations

☒ Enable Protected View for Outlook attachments

Data Execution Prevention

☒ Enable Data Execution Prevention mode

Appendix-D

Software restriction policies (SRP)-windows 7

Type secpol.msc from command prompt, under Software Restriction Policy section, select Additional Rules- > New path rule.

Path if using Windows XP: %UserProfile%\Local Settings*.exe
 Path if using Windows Vista/7/8: %LocalAppData%*.exe
 Security Level: Disallowed
 Description: Don't allow executables to run from %AppData%.

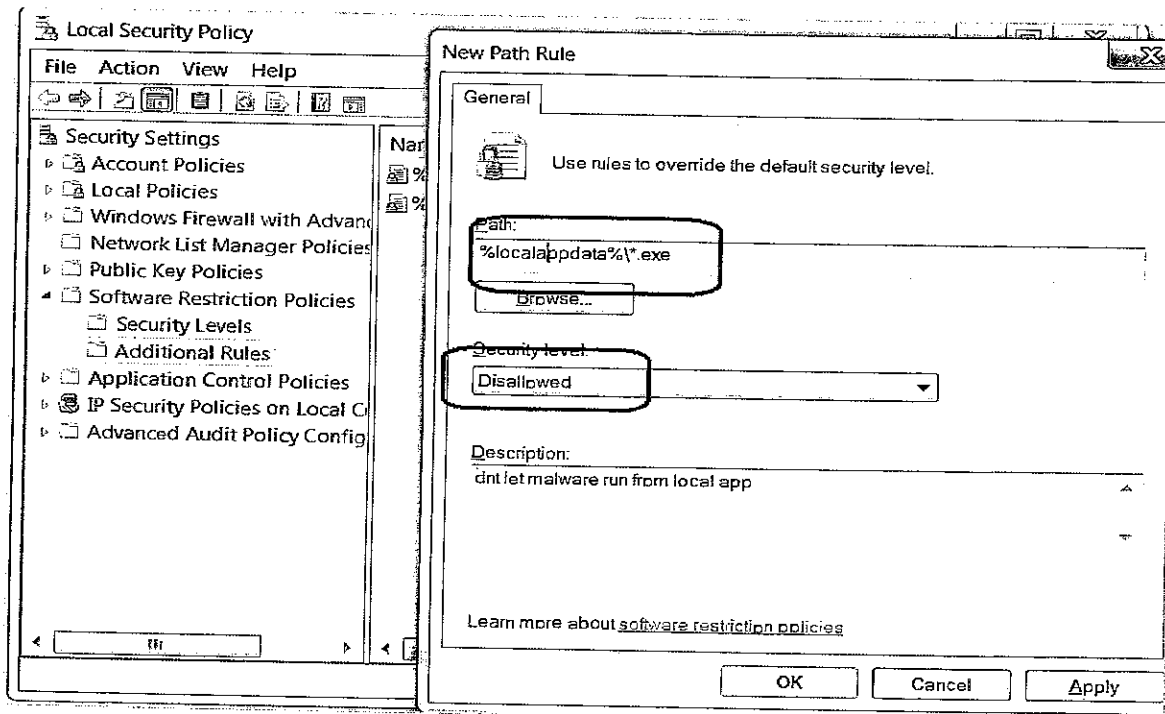


Fig: blocking executables running from %local appdata%

Note: this setting universally prevents exe's running from the said location. This can selectively opted-out by specifying the legitimate application path and give the security level as unrestricted.

Appendix-E

Browser JSGuard

This tool is a browser extension which detects and defends malicious HTML & JavaScript attacks made through the web browser based on Heuristics. It alerts the user on visiting any malicious web pages and provides the detailed analysis threat report of the web page. For more details, see below:

https://cdac.in/index.aspx?id=cs_eps_BrowserJSGuard

Download Links:

For Firefox Web Browser:

<https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/>

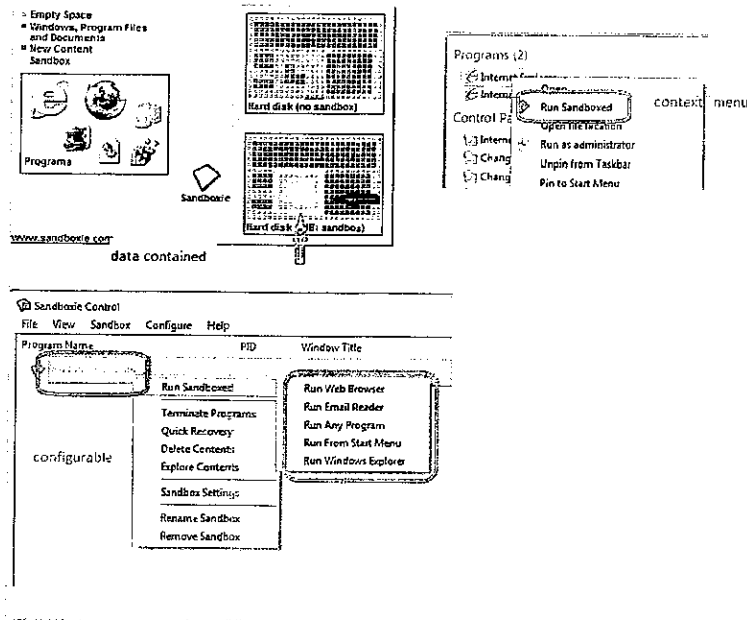
For Google Chrome Web Browser:

<https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb>

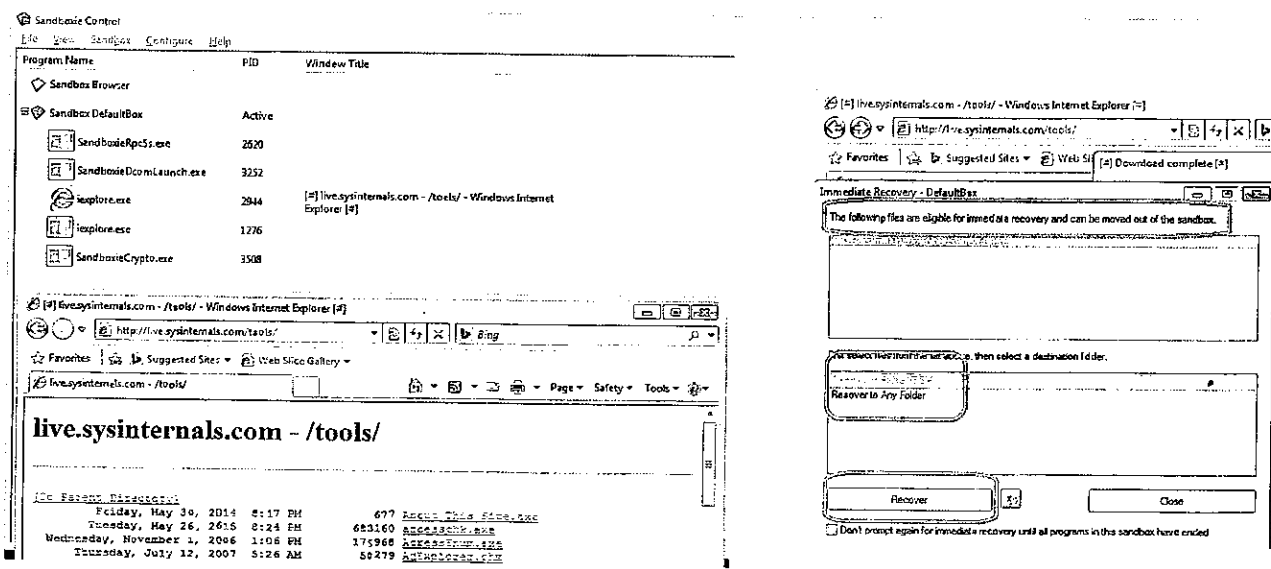
Sandboxing your Browser

A program called **Sandboxie** (<http://www.sandboxie.com/>) which applies the sandbox security concept to protect any browser.

Sandboxie makes surfing the web really secure and safe. You can always be relaxed and be sure that no malware can infect your system. Also, while surfing, various temporary files, cookies, cache, etc, are created and downloaded to the computer. All the aforementioned remain inside Sandboxie and can be easily cleaned by deleting the Sandboxie contents, and without worrying about where to look for them on your computer. Just one click to delete the Sandboxie contents, and it's all gone.



Basically, the protected browser is made to look within a small directory, but it thinks that that directory is drive C. Sandboxie, and any sandbox in general, does not aim to prevent an attack, but instead contains the attack, within that directory. If the attack creates folders and files, it will be created in that directory. If it installs hacking tools and malware, they will all be confined to that directory. All your downloads will also arrive into that directory first, and Sandboxie will help move it back to the outside world. And everything in that directory can be wiped away with one click. In the Unix world, the concept is called chroot, and is traditionally used to prevent compromised server services from affecting the rest of the system. **This program is vital to securing your browser.** The main use of Sandboxie is for surfing the web where it keeps the browser isolated, and the system remains safe from various malware infections.



Right click on the sandbox and choose Sandbox Settings.

- delete->delete invocation> checkmark automatically delete contents of sandbox so that anything that gets into sandbox does not persist on your system
- program stop->leader programs> < your preferred browser> so that anything that gets into this sandbox get terminated when chrome exits
- restrictions->Internet access> <or your preferred browser> so that anything that malware drops onto the system cant access
- restrictions->start/run access> <your preferred browser>
- restrictions->drop rights> checkmark 'drop rights ...'
