



CYBER SECURITY ADVISORY

Recommendations & Best Practices for banks and
other financial sectors

CERT-India

Mitigation Recommendations for Financial Institutions to prevent breaches of Payment Systems

There is a significant rise in cyber security incidents in the country and globally, targeting financial service industries and banks, particularly its ATM driving and switching infrastructure, SWIFT applications and overall ICT infrastructure with the intention of stealing cash or sensitive data.

Based on the nature of incidents and analysis/study thereof, the following security recommendations and best practices are advised to financial institutions for **implementation and compliance**.

- I. Security measures for payment Gateways and ATM driving and switching systems
 - Isolate Payment [ATM/ card processing/ HSM] System network with strict control policies and rigorous monitoring. Implement Multi factor authentication for accessing ATM switch application and other related application server systems.
 - Configure the switch application server to log transactions and preferably route to a centralized logging mechanisms. Routinely rotate, audit transactions and system logs and check for anomalies.
 - 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
 - Regular check on the configuration changes and appropriate usage of configuration and change management. We have observed that the 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

Firewalls, AV gateways, Mail servers, Active Directories and enforcing effective change control policies

- Baseline the regular activities in the ATM Application switch network. Diligently identify behaviors such as unexpected SSH logins, new System Services/ processes, new User account Creations, command history, log in user history, network usages and changes in system configurations.
- Implement adequate and tested network security controls prevent internet hosts from accessing the private network infrastructure servicing your payment switch application server. Deploy Strict firewall policies to check for connections to and from Core- banking network systems /branches /SWIFT / payment gateways etc.
- Develop a baseline of the day to day [/weekly] expected transaction amounts, frequency, and timing and offshore transactions. Monitor and flag anomalous transactions for suspected fraudulent activity. Ensure Close co-ordination with payment processing providers VISA, MasterCard, NPCI etc. for anomalous / bogus transactions and real-time response for those transactions.
- Segmentation between the customer's locally hosted SWIFT infrastructure and its larger enterprise network reduces the attack surface and has shown to be an effective way to defend against cyber attacks which commonly involve compromise of the enterprise network.
- Define a secure Swift Zone to include only SWIFT related components, including the messaging interface, communication interface, SWIFTNet Link, Hardware Security Module, cloud connector, jump server and machines solely dedicated to the operation or administration of the locally hosted.
- SWIFT infrastructure and this zone should only contains software that is necessary to secure, operate, monitor, and manage the secure zone. Non-essential systems or software cannot be located within the secure Zone (for

example, Microsoft Office, e-mail client software, browser applications and other related)

- The users of the SWIFT NETWORK should use Dedicated or restricted methods to access the systems and services. Use physical machines located within the secure zones (that is machines used only for SWIFT purposes or Jump servers, Or from local machine to a separate Virtual Machine (VM) on a central environment in order to access the secure zone having no other software installed, except for the software needed to operate, monitor, and secure it.
- Restrict /block internet access in the SWIFT network such as Any required Internet access is permitted only if initiated in the outbound direction, or to whitelisted sites etc.
- The Windows servers are either 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.
- SWIFT operators must be cautioned social engineering, shoulder surfing, key logger and spear-phishing. Instances of sending fake messages (letters of credit or payments formatted like SWIFT messages) outside of the SWIFT Network were seen. Operators should be taught that SWIFT messages should only be sent over the SWIFT Network. Messages formatted like SWIFT messages outside of the SWIFT Network should not be acted upon
- In an unlikely event, if the SWIFT machines are compromised, additional applications on the system can be further compromised to gain additional access. Instances of Keyloggers, Screen scrappers, Credential dumpers were observed from SWIFT Zones to gain necessary SWIFT credentials. Thus attackers are in a position to locally create, approve and submit messages as any legitimate user would do through the back office or interface applications. Interface Software connecting to the SWIFT network will not flag these messages as fraudulent and attackers and attackers hide evidence by removing some of the traces of the fraudulent messages. Keep in touch with SWIFT for regular updates /IOCs, attack patterns and apply them on your swift network.

- 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
- II. Security measures of overall banking infrastructure including branches
- 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**
 - 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.

- 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.

- **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]

- 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 pushed 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.msdn.microsoft.com/powershell/2015/06/09/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/UseLogon
Credential=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/library/security/2871997#ID0E3D>
- Enforce application whitelisting on all endpoint workstations. This will prevent 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.