Remote File Download via Desktopimgdownldr Utility

edit

Identifies the desktopimgdownldr utility being used to download a remote file. An adversary may use desktopimgdownldr to download arbitrary files as an alternative to certutil.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.process-*
- logs-windows.forwarded*
- logs-windows.sysmon_operational-*
- endgame-*
- logs-system.security*
- logs-m365_defender.event-*
- logs-sentinel_one_cloud_funnel.*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References:

- https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Command and Control
- Resources: Investigation Guide
- Data Source: Elastic Endgame
- Data Source: Elastic Defend
- Data Source: System
- Data Source: Microsoft Defender for Endpoint
- Data Source: SentinelOne
- Data Source: Sysmon

Version: 313

Investigating Remote File Download via Desktopimgdownldr Utility

Attackers commonly transfer tooling or malware from external systems into a compromised environment using the command and control channel. However, they can also abuse signed utilities to drop these files.

The `Desktopimgdownldr.exe` utility is used to to configure lockscreen/desktop image, and can be abused with the `lockscreenurl` argument to download remote files and tools, this rule looks for this behavior.

Note: This investigation guide uses the Osquery Markdown Plugin introduced in Elastic Stack version 8.5.0. Older Elastic Stack versions will display unrendered Markdown in this guide. This investigation guide uses the Investigate Markdown Plugin introduced in Elastic Stack version 8.8.0. Older Elastic Stack versions will display unrendered Markdown in this guide.

Possible investigation steps

- Investigate the process execution chain (parent process tree) for unknown processes. Examine their executable files for prevalence, whether they are located in expected locations, and if they are signed with valid digital signatures.
- Identify the user account that performed the action and whether it should perform this kind of action.
- Contact the account owner and confirm whether they are aware of this activity.
- Investigate other alerts associated with the user/host during the past 48 hours.
- !{investigate{"label":"Alerts associated with the user in the last 48h","providers":[[{"excluded":false,"field":"event.kind","queryType":"phrase","value":"signal","valueType":"string"},{"excluded":false,"field":"user.id","queryType":"phrase","value":"{{user.id}}","valueType":"string"}]],"relativeFrom":"now-48h/h","relativeTo":"now"}}
- !{investigate{"label":"Alerts associated with the host in the last 48h","providers":[[{"excluded":false,"field":"event.kind","queryType":"phrase","value":"signal","valueType":"string"},{"excluded":false,"field":"host.name","queryType":"phrase","value":"{{host.name}}","valueType":"string"}]],"relativeFrom":"now-48h/h","relativeTo":"now"}}
- Assess whether this behavior is prevalent in the environment by looking for similar occurrences across hosts.
- Check the reputation of the domain or IP address used to host the downloaded file or if the user downloaded the file from an internal system.
- Examine the host for derived artifacts that indicate suspicious activities:
- Analyze the file using a private sandboxed analysis system.
- Observe and collect information about the following activities in both the sandbox and the alert subject host:
- Attempts to contact external domains and addresses.
- Use the Elastic Defend network events to determine domains and addresses contacted by the subject process by filtering by the process' `process.entity_id`.

- Use the Elastic Defend registry events to examine registry keys accessed, modified, or created by the related processes in the process tree.
- Examine the host services for suspicious or anomalous entries.
- !{osquery{"label":"Osquery - Retrieve All Services","query":"SELECT description, display_name, name, path, pid, service_type, start_type, status, user_account FROM services"}}
- !{osquery{"label":"Osquery - Retrieve Services Running on User Accounts","query":"SELECT description, display_name, name, path, pid, service_type, start_type, status, user_account FROM services WHERE\nNOT (user_account LIKE *%LocalSystem* OR user_account LIKE *%LocalService* OR user_account LIKE *%NetworkService* OR\nuser_account == null)\n"}}
- !{osquery{"label":"Osquery - Retrieve Service Unsigned Executables with Virustotal Link","query":"SELECT concat(*https://www.virustotal.com/gui/file/*, sha1) AS VtLink, name, description, start_type, status, pid,\nservices.path FROM services JOIN authenticode ON services.path = authenticode.path OR services.module_path =\nauthenticode.path JOIN hash ON services.path = hash.path WHERE authenticode.result != *trusted*\n"}}
- Retrieve the files' SHA-256 hash values using the PowerShell `Get-FileHash` cmdlet and search for the existence and reputation of the hashes in resources like VirusTotal, Hybrid-Analysis, CISCO Talos, Any.run, etc.
- Investigate potentially compromised accounts. Analysts can do this by searching for login events (for example, 4624) to the target host after the registry modification.

False positive analysis

- This activity is unusual but can be done by administrators. Benign true positives (B-TPs) can be added as exceptions if necessary.
- Analysts can dismiss the alert if the downloaded file is a legitimate image.

Response and remediation

- Initiate the incident response process based on the outcome of the triage.
- Isolate the involved host to prevent further post-compromise behavior.
- If the triage identified malware, search the environment for additional compromised hosts.
- Implement temporary network rules, procedures, and segmentation to contain the malware.
- Stop suspicious processes.
- Immediately block the identified indicators of compromise (IoCs).
- Inspect the affected systems for additional malware backdoors like reverse shells, reverse proxies, or droppers that attackers could use to reinfect the system.
- Remove and block malicious artifacts identified during triage.
- Investigate credential exposure on systems compromised or used by the attacker to ensure all compromised accounts are identified. Reset passwords for these accounts and other potentially compromised credentials, such as email, business systems, and web services.
- Run a full antimalware scan. This may reveal additional artifacts left in the system, persistence mechanisms, and malware components.
- Determine the initial vector abused by the attacker and take action to prevent reinfection through the same vector.

```
(process.name : "desktopimgdownldr.exe" or ?process.pe.original_
process.args : "/lockscreenurl:http*"
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Command and Control
  - ID: TA0011
  - Reference URL: https://attack.mitre.org/tactics/TA0011/
- Technique:
  - Name: Ingress Tool Transfer
  - ID: T1105
  - Reference URL: https://attack.mitre.org/techniques/T1105/

« Remote File Copy via TeamViewer

Remote File Download via MpCmdRun »