SquirrelWaffle IOCs List

SquirrelWaffle Loader and Payload SHA1 Hashes:

- de9fc8b4679c66d47fdfa022352e3c279bc4ee2a (email zip)
- fa650a80d51c0aa109292b1dfa23b664bf58a19b (xls)
- 41703e192b233a6fb4eb62a6ba9f371673cbc5e3 (email zip)
- 31caffe4abbfb76a351131059ab97b961556e941 (xls)
- 8d7089f17bd5706309d7c6986fdd1140d6c5b4b2
- 52452f6f0ab73531fe54935372d9c34eb50653d8
- bce0e9e1c6d2e7b12648ef316748191f10ed8582
- 8ba7694017d1cea1d4b73f39479726478df88b20
- 8aec96029b83d3b226c8c83dd90f48946ee97001
- 8262cd7029f943a7b6199b5a6c51ec19e085c3b7
- 75eff4df55a6eb712bce204bbff7b8d69602c572 (email zip)
- 5fcff37a1b9e177fa65e45d9887e3e67d73cd048 (doc)
- 3a631b3df9fca127c30fc94e1dc0190ea2dc7b7d (vbs)
- 55d3d2226a8af0b6cfcfbe8d590cd880954ca419 (dll)
- 65b43bfe8a5f2481d70b76ebd543b9f5b4baa0f6 (cobalt strike)

SquirrelWaffle File IoCs:

- good.good
- good1.good
- good2.good
- test.test
- test1.test
- test2.test
- www1.dll
- www2.dll
- www3.dll
- www4.dll
- www5.dll
- version-1354854470.xls
- chart-1187900052.xls
- diagram-127.doc
- diagram_1017101088.xls
- specification-1001661454.xls
- Pin.vbs
- c:\Datop

ProxyNoShell Reply Chain Email File Logs:

"IPM.BlaBla" string in logs in the following directories:

- %ExchangeInstallPath%\Logging\ConversationAggregationLog
- %ExchangeInstallPath%\Logging\ConversationProcessingLog
- %ExchangeInstallPath%\Transport\Logs\MessageTracking

ProxyNoShell Remote Unauthenticated PowerShell Logs:

- "New-ManagementRoleAssignment" or "New-MailboxExportRequest" cmdlet execution in the logs within the %ExchangeInstallPath%\Logging\CmdletInfra\Powershell-Proxy\Cmdlet directory:
    - AuthenticatedUser is the name of impersonated mailbox user
    - ProcessName contains w3wp
- Check the data field in the logs within the %ExchangeInstallPath%\Logging\LocalQueue\Exchange directory for JSON data with the Operation Key value containing the executed PowerShell cmdlets.

ProxyShell HTTP logs:

- Requests against /autodiscover/autodiscover.json containing “powershell”, “mapi/nspi”, “mapi/emsmdb”, “/EWS” or “X-Rps-CAT”.
    - Successful Exploitation: Status codes 200, 301, or 302
    - Attempted Exploitation: Status Codes 400, 401, or 404

SquirrelWaffle IOCs List

Qakbot File IoCs:

C:\Users\<user>\EmailStorage_<hostname>_<username>_<timestamp>\collector_log.txt

Websites hosting SquirrelWaffle Loader (followed by the following pattern: [a-z]+\.[a-z0-9]+\.com\/[a-z]+\/[a-z]+-[0-9]+)

- virasea[.]ir/
- neginraeisi[.]ir/
- idrispharma[.]com/ (website now down)
- shaheenaasif[.]com/
- stage.the-metaphor[.]com/
- sercoint[.com.bo]/
- sdf.wwkwe[.]com/
- aparnashealthfoundation[.]aayom[.]com/
- abogados-en-medellin[.]com/
- priyacareers[.]com/
- perfectdemos[.]com/
- bussiness-z[.]ml/
- cablingpoint[.]com/
- bonus[.]corporatebusinessmachines[.co.in]/

SquirrelWaffle C2 Domains:

- imperialmm[.]com
- nimixtutorials[.]ir
- 24.229.150[.]54
- grandthump[.co.in]
- arancal[.]com
- perfectdemos[.]com
- bonusvulkanvegas[.]srdm[.]in
- dashboard[.]adlytic[.]ai
- celulasmadreenmexico[.]com[.]mx
- cablingpoint[.]com
- priyacareers[.]com
- ebrouteindia[.]com
- afrizam[.]360cyberlink[.]com
- test[.]dirigu[.]ro
- assurant[.]360cyberlink[.]com
- sig[.]institutoacqua[.]org[.]br
- ifiengineers[.]com
- giasuphire[.]tddvn[.]com
- gerencial[.]institutoacqua[.]org[.]br
- bussiness-z[.]ml

YARA Rules:

- SquirrelWaffle YARA Rule:

```
import "pe"

rule SquirrelWaffle_Loader {

  meta:

    description = "Detects SquirrelWaffle Loader"

    author = "BlackBerry Threat Research Team"

    date = "2021-11-01"

license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"
```

```
  strings:
    $s1 = "true.dll"
    $s2 = "Teachhear"
    $s3 = "RSDSpz"
    $s4 = "Actcause"
    $s5 = "c:\\equal\\True\\bird_Select\\780\\true.pdb"
    $s6 = "AppPolicyGetProcessTerminationMethod"
    $s7 = "LocaleNameToLCID"
    $s8 = "DHCPSAPI.DLL"
  condition:
  (
  //PE File
  uint16(0) == 0x5a4d and
  // dll
  pe.DLL and
  // PE Sections
  pe.number_of_sections == 5 and
  // Checksum is not set and does not match
  pe.checksum != pe.calculate_checksum() and
  //All Strings
  all of ($s*) and
  // Imphash
  pe.imphash() == "1b8854882478e8ab7439d9dedeec9966" )
}
```

- **ProxyShell YARA Rules:**

```
rule EXPL_Exchange_ProxyShell_Failed_Aug21_1 : SCRIPT {
  meta:
```

```
    description = "Detects ProxyShell exploitation attempts in log files"
    author = "Florian Roth"
    score = 50
    reference = "https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html"
    date = "2021-08-08"
    modified = "2021-08-09"
  strings:
    $xr1 = / \/autodiscover\/autodiscover\.json[^\n]{1,300}\/(powershell|mapi\/nspi|EWS\/|X-Rps-CAT)[^\n]{1,400}401 0 0/ nocase ascii
    $xr3 = /Email=autodiscover\/autodiscover\.json[^\n]{1,400}401 0 0/ nocase ascii
  condition:
    1 of them
}
rule EXPL_Exchange_ProxyShell_Successful_Aug21_1 : SCRIPT {
  meta:
    description = "Detects successful ProxyShell exploitation attempts in log files"
    author = "Florian Roth"
    score = 85
    reference = "https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html"
    date = "2021-08-08"
    modified = "2021-08-09"
  strings:
    $xr1a = / \/autodiscover\/autodiscover\.json[^\n]{1,300}\/(powershell|X-Rps-CAT)/ nocase ascii
    $xr1b = / \/autodiscover\/autodiscover\.json[^\n]{1,300}\/(mapi\/nspi|EWS\/)[^\n]{1,400}(200|302) 0 0/
    $xr2 = /autodiscover\/autodiscover\.json[^\n]{1,60}&X-Rps-CAT=/ nocase ascii
    $xr3 = /Email=autodiscover\/autodiscover\.json[^\n]{1,400}200 0 0/ nocase ascii
  condition:
    1 of them
}
```