

Malware Investigation

This report analyses 3 different malware types and plays a role in incident reporting. This report has been created using Sumologic for lab purposes. Previously parsed logs have been used to run the scripts. Considering a role of an SOC analyst, a report has been prepared for malwares – Silentrinity, OrangeWorm and BackOff along with business implications.

Malware 1: Silentrinity

As an SOC analyst, to analyse this kind of malware, I would first filter out all HTTP requests to understand in detail. This would mean looking at their connection type, their status codes, the headers, file data and payloads. Additionally, I would look if there were an .xml file containing code to gather data or any kind of illegal characters that can be found in these details. The analysis tool also provided an HTTP analysis to filter by host, and I would check all requests for the suspicious host. We could also follow the HTTP stream to check the HTTP details in the PCAP file and then use a ladder diagram to understand the conversation that has been established. For this alert, I would set a criticality of **high** for the reason that if the malware convinces the person to click the phishing link, and gets access to the network, it could be undetected for a long period of time and serve as an APT slowly stealing all information from the servers. The dashboards that can be useful to monitor this alert would be endpoint security dashboard to view endpoint activity in case a user clicks on a phishing link, and maybe a threat intelligence dashboard that can be used to get an idea about IOC's for this kind of threat.

For the business, a detection of multiple HTTP requests with a value for file data and payloads can mean exfiltration or infiltration of data. This could mean the business could be impacted with loss of data or loss of trust in customers. Short-term risks involve complete downtime to resolve the issue, or replacement of hardware systems. The long-term risks involve loss of business and loss of financial money if the hardware systems must be replaced completely. This could also raise multiple concerns amongst the users and employees in the long run.

To remediate this incident, first there should be a thorough forensic analysis done on the systems affected, and for any other things that have been noticed as malicious. After this, the systems affected can be replaced or restored, by removing the malware, and then improving security controls that exist currently. Apart from these steps, the incident response plan should be implemented and improvised further by thorough analysis of this malware and other similar versions of the malware, which use similar methods. Employees should be trained and made aware of the malware and how to look out for it and not fall prey to it.

Malware 2: OrangeWorm

As an SOC analyst investigating the OrangeWorm alert, I would start by analysing the TCP results that have been generated by applying filters around tcp. The packets can be then investigated to check for a specific pattern in their communications that may be depictive of the Orangeworm. A pattern like tcp rst/ack packets sent from random port numbers to known port numbers could be one. Additionally, the payloads length could be viewed in this pattern that may be visible. Another thing that could be done would be to evaluate the DNS requests made, by using the dns filter and checking the resolved DNS names to identify random domain names or weird looking ones with extra characters within them. It should be one goal to identify the C2 server to understand the communications more detailed. For this alert, the criticality I would save would be **high** because it affects mainly health institutions which hold very important health information about patients, and even the fact that once it is in the network it spreads quickly onto other devices. One of the dashboards that can be very useful for this investigation can be a traffic analysis dashboard. The one which filters each request by protocol and methods used, along with payload information and traffic trends obtained from the packet capture.

The business implications for this could be very harsh on the whole organization. Since orangeworm aims at healthcare and high-level institutions, the short-term risks could be associates with identity theft, change and alteration of patient data, or stealing of login credentials. These risks extend onto the short-term risks and then will be higher in case as long-term risks which would be death of patients incase of alterations of data, huge financial losses, complete network reset resulting in operational downtime, as well as reputational damage.

For remediation, all the systems should be completed shut down and resetted with proper formatting to ensure the complete removal of the malware after complete analysis of the threat. All credentials for the organization should be changed ensuring a minimum character requirement. Outsourcing can be done to ensure that all systems are patched properly to their latest version, avoiding any open doors for them.

Malware 3: Backoff

An SOC analyst, the first thing to do would be to have a quick glimpse of the different kinds of packets and protocols being used in the PCAP and then analyze them according to the traits that the backoff malware followed. We can first filter out ARP requests, which can show us that either the attacker is trying to gather information about active targets on the network or using lateral movement tactics to move through the network. Another thing to do is to filter out HTTP requests to view if there are any malicious user-agent strings or cache-control. The connection status would also tell us that the attacker is trying to “keep-alive” to avoid sending too many requests. Additionally, UDP packets can be filtered for specify LLMNR or MDNS requests which are used to resolve names further in case the DNS resolver can’t do it. The criticality assigned to this even as per the Threat Analysis is **high**. The malware spreads easily onto other computers into a network and must be prevented from entering the network. The dashboards that can be useful to detect the backoff malware can be a DNS based dashboard to show the correctly resolved DNS and other related things. This would reduce the confusion with other requests that come into the tool.

The short-term risks associated with the backoff malware can be a huge data breach which includes financial number or personal identification numbers or sensitive data like age, race, sex of people and then result in financial or customer confidential information. The long-term risk would be legal consequences of not implementing the correct required tools to avoid this and chances of the malware going undetected for long periods of time, thereby turning to almost an APT, coming with financial losses and increased security costs to the organization.

To remediate this, a honeypot can be set up, which completely allows an attacker to believe it is the correct website they have reached and then use it to learn about the techniques and amount of hackers trying to attack the system. Network segmentation can be implemented, and a DMZ can be used to separate communications as per the organizational structure. Backup and recovery servers should be set up and kept off any kind of internet communications except the time of backing up the important data.

Appendix

Malware 1: Silenttrinity

[illegible][illegible]

Malware: OrangeWorm

CS Enterprise @ cloudshark.org

orangeworm_1hr.pcap 1.8 mb - 7349 packets - more info

tcp

No.	Time	Source	Destination	Protocol	Length	Info
24	18.030750	192.168.99.52	35.221.46.24	TLSv1.2	628	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
25	18.120116	35.221.46.24	192.168.99.52	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
26	18.120161	192.168.99.52	35.221.46.24	TCP	54	63749 → 443 [ACK] Seq=727 Ack=1969 Win=261632 Len=0
27	18.120657	192.168.99.52	35.221.46.24	TLSv1.2	325	Application Data
28	18.173349	35.221.46.24	192.168.99.52	TLSv1.2	194	Application Data
29	18.173393	192.168.99.52	35.221.46.24	TCP	54	63749 → 443 [ACK] Seq=998 Ack=2100 Win=261632 Len=0
31	21.178309	192.168.99.52	167.71.97.235	TCP	55	[TCP Keep-Alive] 49705 → 9200 [ACK] Seq=1 Ack=1 Win=1025 Len=1
32	21.222627	167.71.97.235	192.168.99.52	TCP	66	[TCP Keep-Alive ACK] 9200 → 49705 [ACK] Seq=1 Ack=2 Win=3213 Len=0 SLE=1 SRE=2
34	22.229243	192.168.99.52	167.71.97.235	TLSv1.2	2484	Application Data
35	22.273052	167.71.97.235	192.168.99.52	TCP	60	9200 → 49705 [ACK] Seq=1 Ack=2432 Win=3198 Len=0
36	22.280096	167.71.97.235	192.168.99.52	TLSv1.2	418	Application Data
37	22.330417	192.168.99.52	167.71.97.235	TCP	54	49705 → 9200 [ACK] Seq=2432 Ack=365 Win=1823 Len=0
38	23.194592	35.221.46.24	192.168.99.52	TLSv1.2	85	Encrypted Alert

0000 c4 ad 34 d3 cc 33 00 00 27 3e 93 12 00 00 45 00 ...4..3...'....E.
0010 09 a6 89 89 40 00 00 06 00 00 c0 a8 63 34 a7 47 ...@.....G.G
0020 61 eb c2 29 23 f0 b9 fe ef 1b b0 67 ab d7 50 18 ...a..#.....g..P.
0030 04 01 2d 16 00 00 17 03 03 09 79 00 00 00 00 00Y.....
0040 00 c8 7c 06 87 08 01 65 1a 36 f6 fd 1a 94 69 49 ...[].....e.....
0050 73 21 23 96 c4 1b 96 36 0f 37 f9 14 15 07 b0 52 ...\$W.....6..7.....R
0060 f7 15 6e 66 3c af 10 39 bd 71 00 77 3a 08 4a 54 ...mfc...9...q...J
0070 80 86 ef 91 cc d3 c4 b0 6a a6 5a 19 14 9c c3 7a ...K.....J.....
0080 88 ed 3e 7f 9c 66 20 f9 28 dc 46 d7 fc 08 00F...C.F.....
0090 6e 47 dc b5 f3 bf 1e 73 15 ce 25 0d 0f 94 a5 ...HG.....s...K.....
00a0 51 b0 fd 0f 54 06 07 17 b1 61 1a 7f 47 14 f3 0a ...Q.....k.....6.....
00b0 e9 2f fb e8 82 3c 13 5b 9c 04 71 0f f4 e5 e2C.....[.....Q.....
00c0 96 b1 9d 58 1d a5 9b 48 2e 90 23 dd bb 59 87 8fK.....H.....J.....
00d0 8e fd 94 39 dc 61 93 92 79 0a ce d9 16 20 f3 199...a.....y.....
00e0 45 b3 7f 76 3b 83 20 91 f0 8b 09 4a d3 cf a8 18 ...E...[b.....3.....
00f0 77 ab 09 ab 70 38 87 a8 52 c6 7a 13 4a e8 06 17 ...w...pB...R...J.....
0100 02 3b 16 78 d7 97 5e cf c4 db 6f 10 c5 4d c8 af ...X.....c.....b.....
0110 88 a2 4a b2 a6 11 cd 5c cf 6d 08 52 e2 0e 93 07 ...J.....b.....R.....

orangeworm_1hr.pcap 1.8 mb - 7349 packets - more info

dns

No.	Time	Source	Destination	Protocol	Length	Info
657	336.618751	192.168.99.52	208.67.222.222	DNS	94	Standard query 0xc87 A tile-service.weather.microsoft.com
658	336.619111	192.168.99.52	208.67.220.220	DNS	94	Standard query 0xc87 A tile-service.weather.microsoft.com
659	336.687462	208.67.222.222	192.168.99.52	DNS	200	Standard query response 0xc87 A tile-service.weather.microsoft.com CHAVE wildcard.weather.microsoft.com.edgekey.net CHAVE e15279
663	336.740073	208.67.220.220	192.168.99.52	DNS	200	Standard query response 0xc87 A tile-service.weather.microsoft.com CHAVE wildcard.weather.microsoft.com.edgekey.net CHAVE e15279
876	448.346284	192.168.99.52	208.67.222.222	DNS	83	Standard query 0x5eba A ctldl.windowsupdate.com
877	448.368493	192.168.99.52	208.67.220.220	DNS	83	Standard query 0x5eba A ctldl.windowsupdate.com
879	448.445478	208.67.222.222	192.168.99.52	DNS	336	Standard query response 0x5eba A ctldl.windowsupdate.com CHAVE au-b-shin.trafficmanager.net CHAVE adownload.windowsupdate.nsatc
880	448.447059	208.67.220.220	192.168.99.52	DNS	336	Standard query response 0x5eba A ctldl.windowsupdate.com CHAVE au-b-shin.trafficmanager.net CHAVE adownload.windowsupdate.nsatc
3799	1989.309277	192.168.99.52	208.67.222.222	DNS	97	Standard query 0x1463 A array506.prod.dsp.mp.microsoft.com
3800	1989.325380	208.67.222.222	192.168.99.52	DNS	113	Standard query response 0x1463 A array506.prod.dsp.mp.microsoft.com A 52.184.216.246
3823	1989.186188	192.168.99.52	208.67.222.222	DNS	74	Standard query 0xf772 A login.live.com
3824	1989.213211	192.168.99.52	208.67.220.220	DNS	74	Standard query 0xf772 A login.live.com
3825	1989.210407	208.67.222.222	192.168.99.52	DNS	291	Standard query response 0xf772 A login.live.com CHAVE login.msa.asnidentity.com CHAVE wa.tn.lg.prod.adnsa.trafficmanager.net A 4
3827	1989.262172	208.67.220.220	192.168.99.52	DNS	291	Standard query response 0xf772 A login.live.com CHAVE login.msa.asnidentity.com CHAVE wa.tn.lg.prod.adnsa.trafficmanager.net A 4
3836	1989.335051	192.168.99.52	208.67.222.222	DNS	77	Standard query 0xd9f4 A ocpp.digicert.com
3837	1989.354317	192.168.99.52	208.67.220.220	DNS	77	Standard query 0xd9f4 A ocpp.digicert.com

orangeworm_1hr.pcap 1.8 mb - 7349 packets - more info

tcp.flags.reset == 1 && tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
15	17.234095	192.168.99.52	35.221.46.24	TCP	54	63749 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
59	38.743685	192.168.99.52	35.221.46.24	TCP	54	63749 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
61	38.743849	192.168.99.52	35.221.46.24	TCP	54	63749 → 443 [RST, ACK] Seq=2 Ack=1 Min=0 Len=0
204	116.629404	192.168.99.52	35.221.46.24	TCP	54	63750 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
215	148.740488	192.168.99.52	35.221.46.24	TCP	54	63750 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
253	148.740231	192.168.99.52	35.221.46.24	TCP	54	63751 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
446	231.232309	192.168.99.52	35.221.46.24	TCP	54	63753 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
544	258.737465	192.168.99.52	35.221.46.24	TCP	54	63755 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
546	258.737655	192.168.99.52	35.221.46.24	TCP	54	63754 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
680	345.383174	192.168.99.52	35.221.46.24	TCP	54	63756 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
741	368.740728	192.168.99.52	35.221.46.24	TCP	54	63759 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
743	368.740918	192.168.99.52	35.221.46.24	TCP	54	63757 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
919	436.252315	192.168.99.52	35.221.46.24	TCP	54	63760 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
988	476.746677	192.168.99.52	35.221.46.24	TCP	54	63763 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
982	476.746864	192.168.99.52	35.221.46.24	TCP	54	63763 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
1131	571.355598	192.168.99.52	35.221.46.24	TCP	54	63764 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
1168	588.741478	192.168.99.52	35.221.46.24	TCP	54	63766 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
1170	588.741668	192.168.99.52	35.221.46.24	TCP	54	63765 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
1297	673.272224	192.168.99.52	35.221.46.24	TCP	54	63767 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0
1342	698.743551	192.168.99.52	35.221.46.24	TCP	54	63769 → 443 [RST, ACK] Seq=999 Ack=2141 Min=0 Len=0

0000 c4 ad 34 d3 cc 33 00 00 27 3e 93 12 00 00 45 00 ...4..3...'....E.
0010 00 28 11 b3 40 00 00 06 00 00 c0 a8 63 34 23 dd ...(.@.....C4.
0020 2e 18 f9 03 01 b0 00 fb 26 a8 73 e2 ea 39 14a...9B.
0030 00 00 75 ec 00 00 ...B....

Malware: Backoff

backoff_1hr.pcap 1.4 mb · 6744 packets · [more info](#)

arp

ApplyClearFilters

Analysis ToolsGraphsExportProfile

No.	Time	Source	Destination	Protocol	Length	Info
71	39.977482	PcsCompu_98:67:01	PcsCompu_05:2f:e4	ARP	42	Who has 192.168.99.54? Tell 192.168.99.55
72	39.977797	PcsCompu_05:2f:e4	PcsCompu_98:67:01	ARP	60	192.168.99.54 is at 08:00:27:05:2f:e4
74	40.005026	PcsCompu_05:2f:e4	PcsCompu_98:67:01	ARP	60	Who has 192.168.99.55? Tell 192.168.99.54
75	40.005045	PcsCompu_98:67:01	PcsCompu_05:2f:e4	ARP	42	192.168.99.55 is at 08:00:27:05:2f:e4
94	45.544071	Routerbo_d3:cc:33	PcsCompu_98:67:01	ARP	60	Who has 192.168.99.55? Tell 192.168.99.1
95	45.544084	PcsCompu_98:67:01	Routerbo_d3:cc:33	ARP	42	192.168.99.55 is at 08:00:27:05:2f:e4
226	84.025839	PcsCompu_05:2f:e4	PcsCompu_98:67:01	ARP	60	Who has 192.168.99.55? Tell 192.168.99.54
227	84.025852	PcsCompu_98:67:01	PcsCompu_05:2f:e4	ARP	42	192.168.99.55 is at 08:00:27:05:2f:e4
265	98.063121	Routerbo_d3:cc:33	PcsCompu_98:67:01	ARP	60	Who has 192.168.99.55? Tell 192.168.99.1
266	98.063135	PcsCompu_98:67:01	Routerbo_d3:cc:33	ARP	42	192.168.99.55 is at 08:00:27:05:2f:e4
359	152.572026	Routerbo_d3:cc:33	PcsCompu_98:67:01	ARP	60	Who has 192.168.99.55? Tell 192.168.99.1
360	152.572039	PcsCompu_98:67:01	Routerbo_d3:cc:33	ARP	42	192.168.99.55 is at 08:00:27:05:2f:e4
377	160.460529	PcsCompu_98:67:01	PcsCompu_05:2f:e4	ARP	42	Who has 192.168.99.54? Tell 192.168.99.55
378	160.460877	PcsCompu_05:2f:e4	PcsCompu_98:67:01	ARP	60	192.168.99.54 is at 08:00:27:05:2f:e4

backoff_1hr.pcap 1.4 mb · 6744 packets · [more info](#)

http

ApplyClearFilters

Analysis ToolsGraphsExportProfile

No.	Time	Source	Destination	Protocol	Length	Info
13	13.356989	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
15	13.405889	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK
35	21.499062	192.168.99.55	72.21.81.240	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?5f4801a0e8b3ca44 HTTP/1.1
37	21.517752	72.21.81.240	192.168.99.55	HTTP	346	HTTP/1.1 304 Not Modified
81	40.925963	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
83	40.975718	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK
124	69.435503	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
127	69.482794	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK
270	99.147660	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
272	99.205762	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK
332	128.239304	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
335	128.286092	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK
369	158.209565	192.168.99.55	157.245.128.27	HTTP	513	GET /updates HTTP/1.1
371	158.256140	157.245.128.27	192.168.99.55	HTTP	155	HTTP/1.1 200 OK

[Checksum Status: Unverified]

Urgent Pointer: 0

Timestamps

SEQ/ACK analysis

TCP payload (459 bytes)

Hypertext Transfer Protocol

GET /updates HTTP/1.1\r\n

Accept: */*\r\n

[truncated]Cookie: user=HBMCFIGHFJDIFNOKGNGJGCOFGBGCHWIONJCCPTDKWBAFOKIBPBAWFLFGPIPOKHADMBHEK

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0\r\n

Host: 157.245.128.27\r\n

Connection: Keep-Alive\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://157.245.128.27/updates]

[HTTP request 1/1]

[Response in frame: 272]

0000 c4 ad 34 d3 cc 33 08 00 27 98 67 01 08 00 45 00 ...4.3...'.g...E.

0010 01 f3 85 7b 40 00 80 06 00 00 c9 a8 63 37 9d f5 ...|@.....c7..

0020 80 1b c2 fc 00 50 54 3f 9f d8 5f 38 61 c2 50 18PT?..._Ba.P.

0030 04 00 43 d6 00 00 47 45 54 20 2f 75 70 64 61 74 ...C...GET /updat

0040 65 73 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 es HTTP/1.1..Acc

0050 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6f 6b 69 65 ept: */*..Cookie

0060 3a 20 75 73 65 72 3d 48 42 4d 43 46 49 47 4e 46 : user=HBMCFIGHF

0070 4a 44 49 46 4e 4f 4b 47 4b 4e 4a 47 43 4f 46 47 JDIFNOKGNGJGCOF

0080 42 47 43 48 4e 4f 4e 4a 43 43 50 49 44 4b 4d 42 BGCHWIONJCCPTDKW

0090 41 41 46 4f 4b 4e 42 50 42 41 4d 46 4c 46 47 50 AAFONBPAWFLFGPI

00a0 49 50 44 4f 4b 48 41 44 4d 42 48 45 4b 43 4f 47 IPDOKHADMBHEKCOG

00b0 4e 42 42 47 46 44 47 47 4d 46 43 41 4b 42 4d 45 NBBGFGGHPGCAKBN

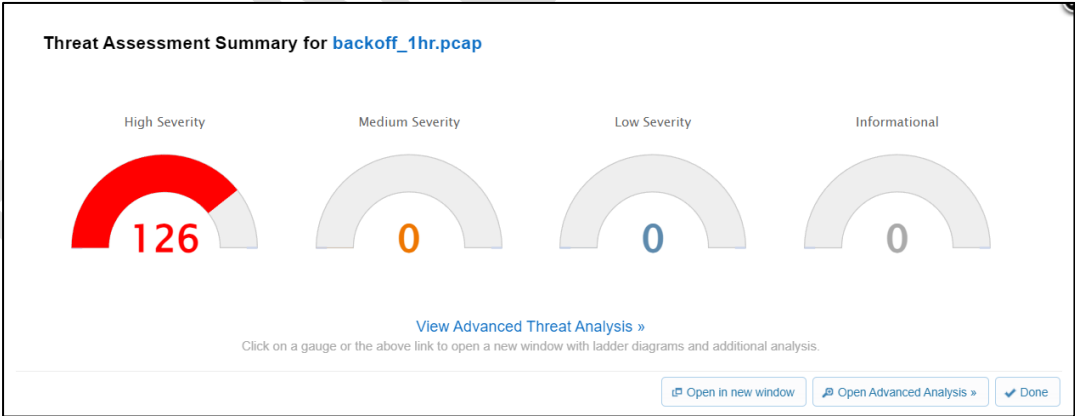
00c0 4e 50 41 4f 44 48 44 41 4c 47 4b 47 4e 48 50 48 NPADODHALGKGNHPP

00d0 4d 4f 4a 45 4f 47 43 49 4d 4c 43 4e 4c 4a 4c 4e NOTFORGETLNCJLJN

00e0 47 41 42 4d 43 4c 4a 4c 4a 4b 49 46 4a 4f 4f 4a GABMCLJLJKIFJOOJ

00f0 44 48 49 4c 44 41 4b 46 4e 4f 4b 46 43 4c 4f 50 DHILDAKFNOKFCLOP

0100 43 44 4b 4b 4b 4b 4b 4b 4b 4b 4b 4b 4b 4b 4b 4b GMLTFCFOWKFEOT



References

1. <https://attack.mitre.org/software/S0692/>
2. <https://blog.f-secure.com/hunting-for-silenttrinity/>
3. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia>
4. <https://symantec-enterprise-blogs.security.com/sites/default/files/2018-04/Orangeworm%20IOCs.pdf>
5. <https://www.cisa.gov/news-events/alerts/2014/07/31/backoff-point-sale-malware>
6. <https://datatracker.ietf.org/doc/html/rfc4795>
7. <https://www.onpointcu.com/blog/why-malware-is-dangerous-and-how-to-protect-yourself-and-your-business/>