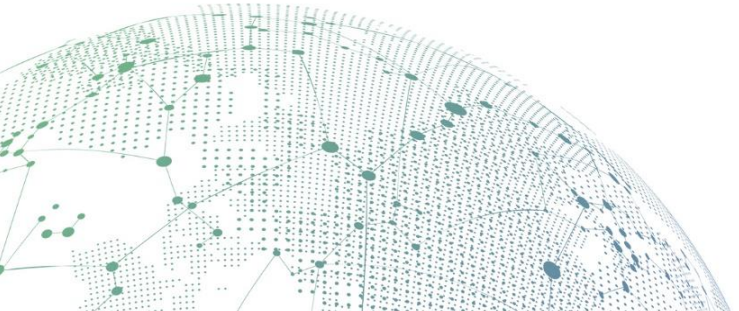
SANGFOR

Sangfor Security Event Processing Method



Content

According to the emergency response experience, the direct phenomenon of customer feedback is generally divide into three types:

1. Webpages being hacked, such as through the device, regulatory unit or customer found himself that being hanged black link(web content such as pornography, drug or gambling), or hanging a webshell, this type is a web-based security issue.
2. Visual anomaly of the host itself such as blue screen (may cause by ransomware or maybe non-security issues such as driver problem), files are encrypted (ransomware), server stuck (Possible mining or program exception).
3. Intermediate traffic anomalies, such as security devices report C&C communications (possibly malicious programs), internal DOS traffic (possibly malicious programs), external network DOS, security device discover vulnerabilities (vulnerability notifications) and so on.

Above coves most of the phenomenon, some case may be combined with the above several scenarios. According to the actual situation analysis, there are some scenes that are not very clear and there may be only a part of botnet logs. No matter which kind, you need to check the following steps before escalate the problem. You can escalate the problem to headquarters.

1 Web-based security issue

Phenomenon:

NGAF home page or key page has been tampered, various bad information or even reactionary information has appeared, or the website has been hijacked to a malicious site.

Troubleshooting:

1. Search the domain name and keywords by search engine, for example: site: sangfor.com and so on. Check on the page to see if it jumps to the black link page.
2. Use the EDR tool to check the abnormal server to see if there any malicious programs and export the kill results.

Information collection before feedback:

1. Abnormality time: Consult the web admin, the approximate time the website was tampered with, such as the time when the administrator found that the website was tempered at around 18/09/2018 1500pm.
2. Host abnormally characteristics: The website was hijacked, accessed through search engine, and hijacked to the gambling site (reported by the regulatory authorities need to provides relevant notification documents)
3. Information and scope of affected hosts: Such as a Windows server with BBS installed has been tempered.
4. Users working hours and account status: If the client normally visits the website from time 0900 to 1730, then after work it should be not able to login.
5. Security device policy configuration: There is a NGAF, NGAF enabled WAF and ISP protections, anti-virus software is installed on the server, and the login method of related security device need to provide.
6. Audit log status: Consult the web administrator about website whether enabled web access log.
7. Provide EDR checking report (EDR report in HTML format).
8. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

Note: If above steps cannot resolved the issue then provide a remote session (If direct provide customer contact information to headquarters' security service, they have the right to refuse to apply for remote. All security service needs remote, this will not describe later).

2 Ransomware

Phenomenon:

Files on the server or PC is encrypted and the extortion information is prompted.

Troubleshooting:

1. Troubleshoot the suffix of the encrypted file in the host.
2. Use ***everything*** to search for the suffix name associated with the ransomware and find the file with the earliest modification time.
3. Use EDR botnet tool to check the abnormal server and run the NSA detection tools to see if there MS17-010 vulnerability patch.

4. **eventvwr** check security logs to see is it been deleted.

Information collection before feedback:

1. Abnormality time: Time that file has been encrypted.
2. Host abnormally characteristics: The suffix of the encryption file.
3. Information and scope of affected hosts: Such as 1 windows server has been encrypted.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF and ISP protections, anti-virus software is installed on the server, and the login method of related security device need to provide.
5. Audit log status: The security log has not been deleted.
6. Provide EDR botnet checking report and check is the MS17-010 vulnerability patch already installed or not.
7. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

3 Ransomware variant

Phenomenon:

Blue screen appears on large amount of server.

Troubleshooting:

1. Run the NSA detection tool to check is MS17-010 vulnerability patch is installed or not.
2. Check task manager, whether has **mssecsvc2.0** process or not.
3. Check if there is a **C:\Windows\qeriuwjhrf** file.
4. Use DER botnet tool to check the abnormal server.

Information collection before feedback:

1. Abnormality time: The server has a blue screen time.
2. Host abnormally characteristics: Blue screen appear on the server.
3. Information and scope of affected hosts: Such as 2 windows server have blue screen.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF and ISP protections, Anti-virus software is installed on the server, and the login method of related security device need to provide.
5. Provide DER botnet checking report and check is the MS17-010 vulnerability patch already installed or not.
6. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

4 Mining virus

Phenomenon:

Server CPU status is high, abnormal process occupy CPU for a long time, and NGAF botnet detects abnormal communication.

Troubleshooting:

1. Use DER botnet tool to check the server.
2. Using process hacker to find suspicious processes and their network connection behavior according to CPU usage ranking.
3. In Virustotal or ThreatBook, check the domain name or IP address of successful connection ether has the characteristics of mine pool.

Information collection before feedback:

1. Abnormality time: Time that administrator found the problem on the server.
2. Host abnormally characteristics: Server CPU abnormal.
3. Information and scope of affected hosts: Such as 1 windows server abnormal.
4. Security device policy and configuration: There is a NGAF, NGAF enabled WAF, APT and IPS, configuration on NGAF is normal, Tencent Manager Anti-virus has installed on the server and the login method of related security device need to provide.
5. Provide EDR botnet checking report.
6. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

Note: When the mining problem is escalate to the security service department, the virus must be in active period. If there is abnormal traffic, then it can be escalate. If there is no abnormal traffic, it is recommended that the customer monitor first then dispose when there is traffic.

5 Malicious program

Phenomenon:

1. Phenomenon1: Host 3389 remote desktop will suddenly drop during use, jump out to the Windows login interface and login again will prompt the remote desktop is busy.
2. Phenomenon2: Found that the host has abnormal communication behavior on NGAF botnet.
3. Phenomenon3: The server has abnormality such as stuck, high memory usage, slow web browsing and large number of network connection that cannot be released.

Troubleshooting:

1. Check related security devices to confirm whether there is any related abnormal communication.
2. Use Wireshark or Colasoft capture packets, capture abnormal traffic.
3. Use EDR botnet tools to check the abnormal server.

Information collection before feedback:

1. Abnormality time: Time that administrator found the problem on the server.
2. Host abnormally characteristics: Server CPU abnormal, high usage of memory, NGAF found botnet.
3. Information and scope of affected hosts: Such as 2 Windows server have problem.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF, IPS and APT protections, configuration is normal, Anti-virus is installed in the server and the login

method of related security device need to provide.

5. Provide EDR botnet checking report.
6. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

Note:

1. When there is traffic problem need to escalate to security service department, the abnormal host must be in the active period. If there is abnormal traffic then it can be escalated. If there is no abnormal traffic, it is recommended that the customer monitor first and then dispose when there is traffic.
2. If during troubleshooting process found that it is non-security issues in phenomenon 3, it required solved by the user site maintenance person.

6 Internal abnormal traffic

Phenomenon:

Security device such as NGAF found abnormal internet traffic, such as traffic spikes, host access to malicious domain name, intranet ARP attacks, intranet flood attacks, intranet port scanning, host-to-public network initiate a lot of scanning and etc.

Troubleshooting:

1. Check the NGAF to find the problematic host for outgoing abnormal traffic.
2. Use EDR botnet tool to check the abnormal server.
3. Use process hacker to check suspicious process and their network behavior.

Information collection before feedback:

1. Anomaly time: Time that administrator found the problem on the server.
2. Host anomaly characteristics: Such as if the address (domain name) accessed by the host is marked as malicious by Virustotal or the host initiates a large number of scan on the public port.
3. Affected host information and scope: Such as 1 windows server, 1 windows 7 PC has problems.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF, ISP and APT, configuration is normal, Tencent Manager Anti-virus has installed on the server and the login method of related security device need to provide.
5. Provide EDR botnet checking report.
6. Provide abnormal host traffic packets.
7. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

Note:

1. When there is traffic problem need to escalate to security service department, the abnormal host must be in the active period. If there is abnormal traffic then it can be escalated. If there is no abnormal traffic, it is recommended that the customer monitor first and then dispose when there is traffic.
2. Abnormal traffic event may cause by P2P download or user uses the agent software. If non-security problem is found during the troubleshooting, it required solved by the user site

maintenance person.

7 Internal DOS

Phenomenon:

Security device such as NGAF discover that internal network host sends a large amount of traffic, causing the user network fail and the network device and the host device to be down.

Troubleshooting:

1. Login to the NGAF and find the host that sends a large number of abnormal packets.
2. Use Wireshark or Colasoft to capture abnormal traffic and analyze.
3. Use EDR botnet tool to check the abnormal server.

Information collection before feedback:

1. Anomaly time: Time that administrator found the problem on the server.
2. Host anomaly characteristic: If the host scans a large number of hosts on the intranet then other hosts on the intranet are down.
3. Affected host information and scope: Such as 1 windows server, 3 windows 7 PCs abnormal.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF, IPS and APR protection, configuration is normal, Tencent Manager Anti-virus is installed on the server and PC, and login method of related security device need to provide.
5. Provide EDR botnet checking report.
6. Provide packets of abnormal host.
7. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

8 Vulnerability notification

Phenomenon:

Client was notify by superior regulatory authority that there were black link, webshell on the website and there was abnormal traffic at the network exit.

Troubleshooting:

1. If the notification is about back link or webshell event, FAE will need to verify whether is a false positive according to the content provided by the report and use Sangfor webshell tool to check the server's files.
2. If the notification is abnormal traffic, FAE will need to use the EDR botnet tools to check according to the report content.

Information collection before feedback:

1. Provide the notification document by superior regulatory authority, direct capture it.
2. Provide what investigations and conclusion that have been done only problems that cannot determined after FAE filtering are accepted.
3. Provide remote method of the related abnormal server.

4. Put the common application emergency troubleshooting toolkit into the host that need to troubleshoot.

Note: If the content of the notification is only for the external attack of the client's public network server and there is no evidence that the intrusion is successful, the security tram will not depose of it because the server will be subject to various scans when it is open to the public network. For such problems, FAE will need to explain to the customer.

9 Other security problem

Phenomenon:

Problems and anomalies phenomenon that are not within the scope of above description.

Troubleshooting:

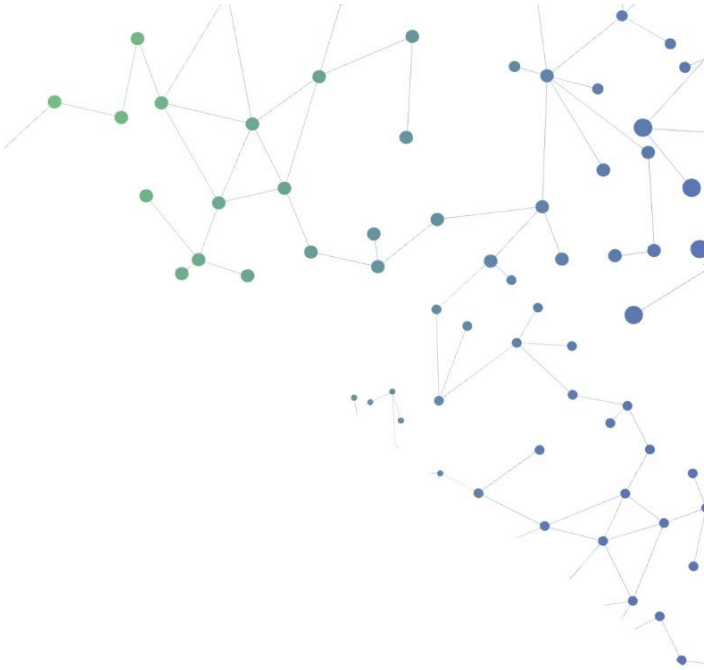
1. Use EDR botnet tool to check the abnormal server.

Information collection before feedback:

1. Abnormal time: Time that administrator found the problem on the server.
2. Host anomaly characteristic: Such as the host scans a large number of hosts on the intranet cause other hosts on the intranet are down.
3. Affected host information and scope: Such as 1 windows server, 3 windows 7 PCs abnormal.
4. Security device policy and configuration: There is a NGAF, NGAF is enabled WAF, IPS and APR protection, configuration is normal, Tencent Manager Anti-virus is installed on the PC, and login method of related security device need to provide.
5. Provide EDR botnet scanning report.
6. Provide packets of abnormal host.
7. Investigation and conclusion that have been made: Process have been done, network connection and no abnormalities have been found.
8. Put the common application emergency troubleshooting toolkit into the server that need to troubleshoot.

Download link for related tools

1. **Sangfor AntiBot:** http://go.sangfor.com/edr-tool-20180824
2. **Colasoft :** https://www.colasoft.com/capsa-free/
3. **Common application emengency troubleshooting toolkit:**
   https://drive.google.com/open?id=1H-LiJypMvSO2HTjdfjC9bjMOK1ZccYjg



SANGFOR