FireEye - advisory

Insight report

Author: Security Advisory Services

Issue: v1.0

13 December 2020

Disclaimer

This document is provided for information purposes only. BT accepts no responsibility for any errors or omissions that it may contain.

This document is provided without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall BT be liable for any claim, damages or other liability (either direct or indirect or consequential), whether in an action of contract, tort or otherwise, arising from, out of or in connection with this document or the contents thereof.

Copyright

Contents

1 Security Advisory Services

We offer strategic security guidance and solutions to organisations across the globe, reflecting the market demand for expert guidance to navigate today's complex cyber security landscape. The practice assists organisations at all stages of their security journey to assess and test their defences and select the solutions that match their security needs.

1.1 Document purpose

This advisory has been produced as a guidance document in relation to the information recently released by FireEye in a blog on their website and it relates to the report that they have been the victim of a cybersecurity incident.

Blogs named:

- Unauthorized Access of FireEye Red Team Tools

https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

- FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

This advisory presents a consolidated analysis of the situation by subject matter experts within the BT Security Advisory teams and is not a reflection of all threats against a, or any, specific organisation.

2 Executive summary

As reported by many mainstream and industry specific media, on 8 December 2020, Kevin Mandia, CEO of FireEye released a blog entry which provided high level details of a cyber security incident affecting their organisation. As part of this blog, it highlighted the loss of several "Red Team" technologies that haven't been previously released in their existing Open Source penetration testing tools.

The FireEye blog entry further reports that no customer details were compromised, and all materials lost were part of the Red Team technology engagements. This further suggests no customer environments and no technology from FireEye is materially affected by the incident.

FireEye has made available a number of security detection signatures to help detect if these stolen Red Team tools may be used against them in future malicious attacks.

Other best practices, such as a focus on patching known vulnerabilities and maintaining vigilance for security alerts and events can help organisations defend themselves.

The effective implementation and use of security controls can be critical to helping defend and detect against adversaries at a time when cyberattacks are becoming more sophisticated.

If your organisation is being affected or you're worried it could be soon, please reach out to us or your account team.

Whether it's practical help or reassurance that you're doing the right thing, we're here to help.

2.1 Overview of the attack

FireEye reported that the attack "used a novel combination of techniques not witnessed by our partners." The blog goes on to report that they were ''witnessing an attack by a nation with top-tier offensive capabilities' and comments that the attack vectors used haven't been seen before by them.

FireEye has released signatures to detect the post-exploitation communications, which include variants of Cobolt Strike controllers, Kerberos traffic and SMB messaging.

FireEye has confirmed that No 'Zero Day' vulnerabilities were leaked. (i.e. no vulnerabilities which are currently unknown to security researchers).

There is also no indication from them that any customer data was compromised.

FireEye is working with a high-grade incident responder to ensure the full details are understood. However, all the details of what occurred have not been publically confirmed at this stage.

2.2 Future considerations

It's acknowledged that investigations into complex data breaches can take months to complete, so it's important to keep a watching brief on this incident, especially if you're a user of FireEye services, in case the scope of the incident changes.

Nation state and sophisticated actors have stolen cyberattack tools from intelligence and cybersecurity organisations before (though not previously from FireEye as far as we know) and made them available publicly[1].

Although attribution or responsibility hasn't yet been made and although the FireEye tools haven't yet been released, it would be consistent with previous events where actors have sold or published stolen assets for financial gain, bragging rights, or in order to embarrass the company and promote public challenge against research into cybersecurity. Given the lack of zero-day exploits being acquired, it's likely that the publication of these FireEye tools would potentially raise the ability of low to middle tier malicious actors.

It's recommended that the FireEye published detection rulesets are utilised within all organisation's detection capabilities. There's a moderate risk that these techniques and technologies will end up in the cybercrime environment and be used as common place communication options.

Defence in depth logic is still as relevant as ever in reducing the spread across an organisation.

It also brings into light the importance of having a well-structured Threat Detection Engineering process in place and ideally, a tried and tested incident response plan ready to go should the worst happen. As FireEye is currently releasing the necessary detection logic to enable companies to correctly update their threat detection capabilities with logic that enables the identification of the communication traffic, being able to respond and deploy these quickly is going to be of high importance.

Further information is available in our Intelligence brief.

2.3 Advice

Whilst details on the attack are limited now, some good practices can be implemented to minimise risks to all organisations:

- install the FireEye detection signatures into threat detection and control infrastructure as rapidly as possible.
- a robust patching and vulnerability management process can help significantly in closing the mechanisms which attackers and malware exploit

[1] https://en.wikipedia.org/wiki/The_Shadow_Brokers

- segmentation of the network is an important step to prevent an attacker or malware moving laterally without triggering alerts or events
- a well-tested incident response plan and possibly a retained response capability can help significantly in reducing the impact of an attack and recovering more rapidly
- focus on gaining telemetry from estates with well-written detection rules and use-cases to handle any scenarios
- understanding assets is critical to understand what may be targeted in any attack and importantly what may be taken or stolen
- enabling of auditing and monitoring of access to systems and data can help with forensic analysis during an incident and can help significantly in reducing the Mean Time To Respond (MTTR).
- incident scenario testing is critical as part of a day-to-day operation to ensure "muscle memory" when any major event occurs – incident or otherwise.

2.4 Appendix

The details of the breach released thus far are contained in three web posts (two FireEye blog and one GitHub signature and CVE posting). The breakdown of the specific items in the blog posts are as follow:

- On 8 December 2020, the security company FireEye reported via the blog section of their website that they had been the victim of a cybersecurity incident
- The blog reports that the attack "used a novel combination of techniques not witnessed by us or our partners in the past," and goes on to assert that the expertise involved in the attack would infer a sophisticated nation state actor
- However, no firm attribution has been made in the official release thus far
- FireEye report that the attackers do not appear to have exfiltrated customer data although they do refer to the attacker having some access to an unspecified set of servers
- The blog goes onto report that the attacker has accessed and exfiltrated a number of their offensive penetration and testing tools (referred to as Red Team tools) which they routinely use to help clients test their security defences and counter measures
- These Red Team tools are reported to have been largely publicly available to some customers of FireEye and include common industry tools associated with Red Team activity
- Based on a limited technical update and GitHub upload from FireEye it would appear that the tools did include custom modifications to help them evade detection by traditional tooling
- Via the GitHub software platform FireEye has released some details as to what their tools sought to exploit, and they have released detection / signatures files to help organisations detect and prevent the use of the tools against them

- From the comments added by FireEye into the GitHub release it would appear that a number of the tools sought to exploit known and documented vulnerabilities – further highlighting the importance of patching and robust vulnerability management as a protection strategy
- Importantly, FireEye has clearly stated that no 'Zero Day' vulnerabilities were leaked. (i.e., no vulnerabilities which are currently unknown to security researchers) and there is no indication that any customer data was compromised
- FireEye report that they are working with partners – including the US FBI and Microsoft - to fully investigate the incident.

The details of the FireEye Blog can be found here:

- https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

Further information here:

- https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

The tools:

- https://github.com/fireeye/red_team_tool_countermeasures

13 December 2020

Find out more at bt.com

Offices worldwide

Registered office: 81 Newgate Street, London EC1A 7AJ

Registered in England No. 1800000