Threat Intelligence

Intelligence assessment: FireEye data breach

Document title:	Intelligence assessment: FireEye data breach		
Document number:	INT_5351	**Date issued:**	09 December 2020
Scope:	This report provides an assessment of the change in threat to BT, and BT's customers, in light of the breach of Penetration Testing tools from FireEye in a recent attack.		
Customer:	BT Internal, BT CTI Customers, Others as appropriate		
Handling:	**TLP: GREEN**		
Actively exploited:	N/A		
Risk rating:	Low to Moderate		

1. Summary

On 8 December, FireEye reported that some tools, which are used after the initial exploitation on an intrusion or red team exercise, were exfiltrated from their estate. There is no indication that any customer data was compromised, or any reason to doubt that the integrity of threat data that FireEye provides to clients is compromised. There is no indication that the attacker is in a position to intercept communications to or from FireEye.

The implications of this attack on the security of BT, and its clients, are assessed to be low. The tools taken appear to be standard pen testing tools designed to replicate existing threat actor behaviours, and as such, they do not represent a significant increase in threat actor capability. Furthermore, FireEye has provided a comparatively simple mechanism to effectively mitigate the threat.

It is assessed as likely that the attack was conducted by a Russian state-sponsored group.

2. How did the attack occur?

FireEye reported that the attack "used a novel combination of techniques not witnessed by us or our partners in the past." No further details on the attacker's tactics, techniques and procedures (TTPs) are in the public domain at the present time.

3. What data was exfiltrated?

Some tools, which are used after the initial exploitation on an intrusion or red team exercise, were leaked. These tools are 'command and control tooling' which avoids standard detection, and tools used for interacting with a windows domain, also focussed on avoiding standard detection techniques. In many instances, these tools had been modified to use obfuscated traffic or to avoid common detection capabilities which therefore makes them more effective than simple proof-of-concept exploit code, or the base attack tools from which they were derived. 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.

4. Who was responsible for the attack?

Our Cyber Threat Intelligence (CTI) analysts assess it highly likely that this attack was conducted by a Russian state sponsored attacker. FireEye has stated that the attack was conducted by a "highly sophisticated state-sponsored attacker".

Some sources have speculated that the attack may be the work of hackers, extracting 'revenge' on FireEye for unspecified legal actions against them. Our analysts have no intelligence to support or refute this hypothesis.

No public claim or responsibility – credible or otherwise – has been made to date.

5. What are the implications for BT, and our customers?

BT and some of our customers could potentially be targeted with FireEye's pen testing tools. Working on the premise that the attacker was a nation state, most probably Russia, the organisations most likely to be targeted are as follows:

- Government entities which hold information of intelligence value to Russia. For example:
  - Ministries of Defence
  - Foreign Offices / Ministries of the Exterior
- Private sector entities which hold valuable intellectual property. The following sectors are assessed to be the most likely to be targeted for this reason:
  - Defence and aerospace
  - Technology
  - Energy
- Public and Private sector organisations which hold data which could assist current Russian cyber-enabled influence operations. Key targets in this category include:
  - Political organisations (think: DNC hack).
  - Organisations holding sensitive personal data (e.g. organisations holding criminal records data, organisations such as niche sex / dating websites).
- Infrastructure targets in countries in which Russia is currently engaged in cyber-enabled sabotage operations. Key targets here are SCADA / Industrial Control Systems (ICS), particularly where deployed in the following fields:
  - power generation and distribution.
  - utilities provision (drinking water, waste water treatment, etc).
  - traffic management / public transport systems.

It is assessed as likely that these penetration tools will be placed into the public domain at some stage – possibly in the very near future (<48hrs). In the event that this happens, they are likely to be leveraged very quickly to launch Ransomware attacks. With regards to the likely ransomware targeting:

- ransomware targeting is largely opportunistic
- the larger the company, the more attractive it is a target for ransomware
- as new TTPs are included into Ransomware-as-a-service offerings, the threat quickly spreads to smaller organisations.

There is currently no indication that the attackers remain on the FireEye network. There is currently no indication that the attackers are in a position to intercept communications between FireEye and their customers / partners. There is currently no indication that the attackers have been able to affect the availability or integrity of threat data which FireEye provides to clients.

6. Recommendations

For existing clients, we will undertake a historic Threat Hunt within your 'live' SIEM logs (<35 days) for evidence of the IOCs detailed within the Intelligence Alert above and provide a summary report detailing our findings.

For existing clients, we will review existing SIEM rules in place and make necessary adjustments to mitigate against the threats detailed within the Intelligence Alert above.

We recommend that all other organisations should deploy the rules provided by FireEye on SIEM solutions to detect and prevent the use of tools / TTPs deployed by FireEye's Red Team. These rules can be found here: https://github.com/fireeye/red_team_tool_countermeasures

Companies engaged in Penetration Testing and Red Teaming should conduct a holistic review of protective mechanisms to ensure that in-house developed tools and expertise is adequately protected.

Our analysts are not advising BT (or our customers) to block email traffic from FireEye (as there is no indication that this is current concern) however increased vigilance is recommended.

Our analysts are not advising BT (or our customers) to assume that the availability or integrity of cyber threat information provided by FireEye is compromised.

7. Ongoing intelligence requirements

The following intelligence requirements remain extant, with our Cyber Threat Intelligence team maintaining a watching brief.

- What were the attacker's 'unique' tactics, techniques and procedures (TTPs) which allowed them to gain access to FireEye?
- Are there any indications that the data breach went beyond Red Team / Pen Testing tools?
- Is any of the breached material (tools, scripts, documents, etc) publicly available?
- Is there any further evidence around likely attribution?
- Is there any evidence of FireEye's Red Team's TTP's being actively deployed by attackers?

In the event that further information is received which significantly alters this assessment, an update to this report will be issued.

If you have any additional intelligence requirements in relation to this incident, please contact cyber.intelligence@bt.com

8. Appendices

Mitre ATT&CK Threat Coverage

Appendix 1 to INT_5351
Dated 09 December 2020

The Mitre ATT&CK techniques associated with specific elements of the breached FireEye toolset are as follows:

MSBUILDME:

- Defense Evasion, Privilege Escalation: T1055.004 – Process Injection: Asynchronous Procedure Call.

PGP:

- Defense Evasion: T1218.004 – Signed Binary Proxy Execution: InstallUtil

SAFETYKATZ:

- Credential Access: T1003.001- OS Credential Dumping: LSASS Memory
- Credential Access and Technique(s): T1003.002 – OS Credential Dumping: Security Account Manager

Risk matrix

Appendix 2 to INT_5351
Dated 09 December 2020

There are 4 categories of risk:

- CRITICAL
- HIGH
- MODERATE
- LOW

Risk ratings are assessed based on the IMPACT that the threat poses against the LIKELIHOOD of the threat occurring. The application of the risk matrix is the same for each of the types of risk e.g. malware, hacktivism etc, so therefore the criteria under each category of IMPACT and LIKELIHOOD takes into account the differences in these crime types.

		LIKELIHOOD			
		UNLIKELY (0-24%)	POSSIBLE (25-59%)	LIKELY (60-89%)	ALMOST CERTAIN (90-100%)
		Downward trend Low number of actors Low number of victims Low opportunity Fluid / disorganised membership Unknown motivation Lack of skill / resource No known exploit	Emerging / continuing trend Low number of prolific individuals Low number of victims Little opportunity Display structure and competence Potentially motivated actor / group Some use of skill / resource Exploit skill required - difficult	Continuing trend High number of individuals High number of victims Medium Opportunity Display structure and competence Well motivated actor / group Use of skill and resource availability - some use of specialists Exploit skill required - moderate to easy	Increasing trend / seasonal High number of prolific individuals High number of victims High opportunity Highly organised, discliplined Highly motivated actor / group Expert skill and resource availability inc corruption / coercion Exploit skill required - automated
IMPACT		Vulnerability risk inside the network - risk of exposure / local availability	Vulnerability risk inside the network - local access / local priviledged	Vulnerability risk outside the network - remote availability / remote access	Vulnerability risk outside the network - remote priviledged
LOW	Low impact on brand / reputation / share price affecting Low threat of public disorder impact Low financial risk Mitigation / patches available Low impact on service delivery	LOW Minor concern	LOW Minor concern	LOW Minor concern	MODERATE Intermediate concern
MODERATE	Moderate impact on brand / reputation / share price affecting Moderate threat of public disorder impact Moderate financial risk Moderate impact on service delivery Mitigation / patches available and / or difficult to implement	LOW Minor concern	MODERATE Intermediate concern	MODERATE Intermediate concern	MODERATE Intermediate concern
HIGH	High impact on brand / reputation / share price affecting High threat of public disorder impact High financial risk Mitigation / patches not yet available High impact on service delivery	LOW Minor concern	MODERATE Intermediate concern	HIGH Significant concern	HIGH Significant concern
VERY HIGH	Critical impact on brand / reputation / share price affecting Critical threat of public disorder impact Critical financial risk Mitigation / patches not yet available, inc 0-day Critical impact on service delivery Threat to life	MODERATE Intermediate concern	MODERATE Intermediate concern	HIGH Significant concern	CRITICAL

Offices worldwide
The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.