The Blockbuster Saga Continues

researchcenter.paloaltonetworks.com/2017/08/unit42-blockbuster-saga-continues/

Anthony Kasza August 14, 2017

By Anthony Kasza

August 14, 2017 at 5:00 AM

Category: Malware, Unit 42

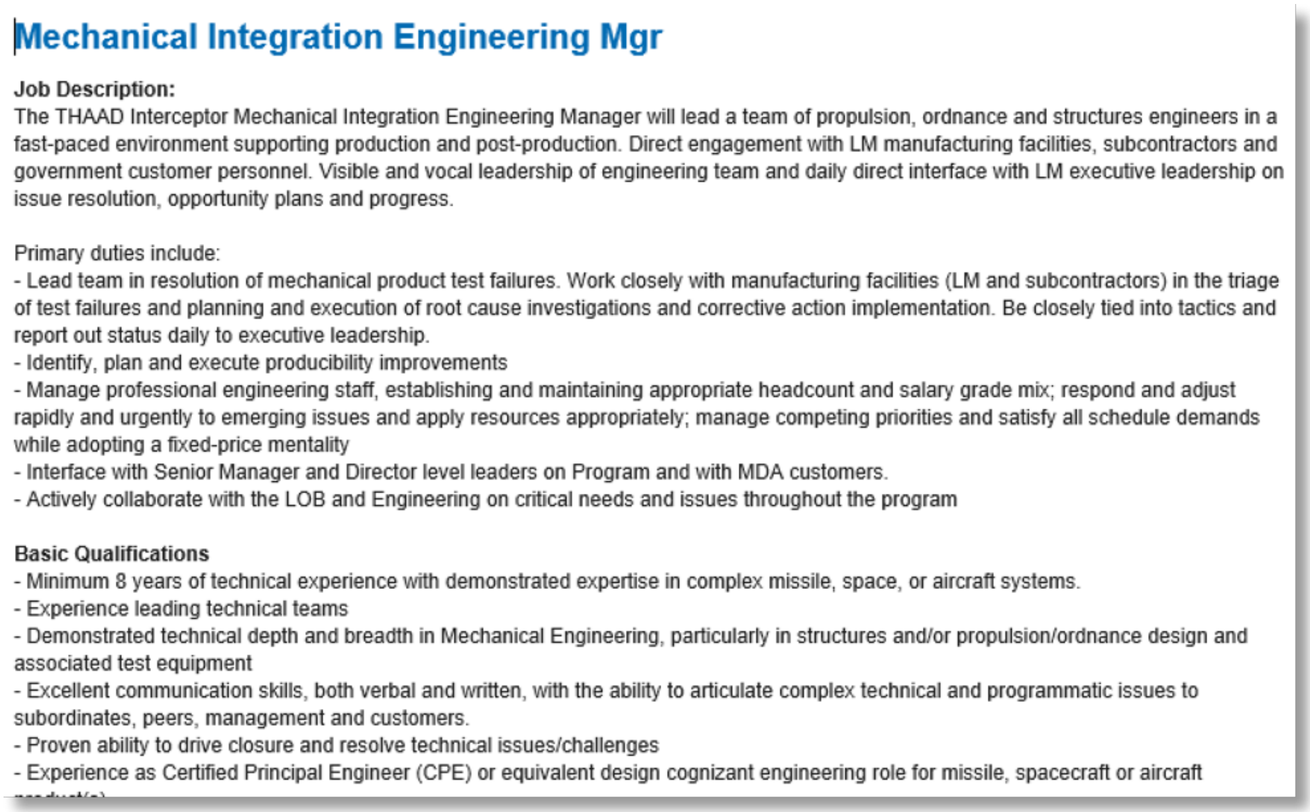
Tags: AutoFocus, Blockbuster, Korea, Lazarus Group, spearphishing

Unit 42 researchers at Palo Alto Networks have discovered new attack activity targeting individuals involved with United States defense contractors. Through analysis of malicious code, files, and infrastructure it is clear the group behind this campaign is either directly responsible for or has cooperated with the group which conducted Operation Blockbuster Sequel and, ultimately, Operation Blockbuster (originally outlined by researchers from Novetta). The threat actors are reusing tools, techniques, and procedures which overlap throughout these operations with little variance. Attacks originating from this threat group have not ceased since our previous report (from April of 2017) and have continued through July of 2017.

New Activity

Recently, we've identified weaponized Microsoft Office Document files which use the same malicious macros as attacks from earlier this year. Based on the contents of these latest decoy documents which are displayed to a victim after opening the weaponized document the attackers have switched targets from Korean language speakers to English language speakers. Most notably, decoy document themes now include job role descriptions and internal policies from US defense contractors.

The following image shows the content of one of the recent decoy documents (de2d458c8e4befcd478a0010789d80997793790b18a347d10a595d6e87d91f34). It is a job description at a defense contractor.



Mechanical Integration Engineering Mgr

Job Description:

The THAAD Interceptor Mechanical Integration Engineering Manager will lead a team of propulsion, ordnance and structures engineers in a fast-paced environment supporting production and post-production. Direct engagement with LM manufacturing facilities, subcontractors and government customer personnel. Visible and vocal leadership of engineering team and daily direct interface with LM executive leadership on issue resolution, opportunity plans and progress.

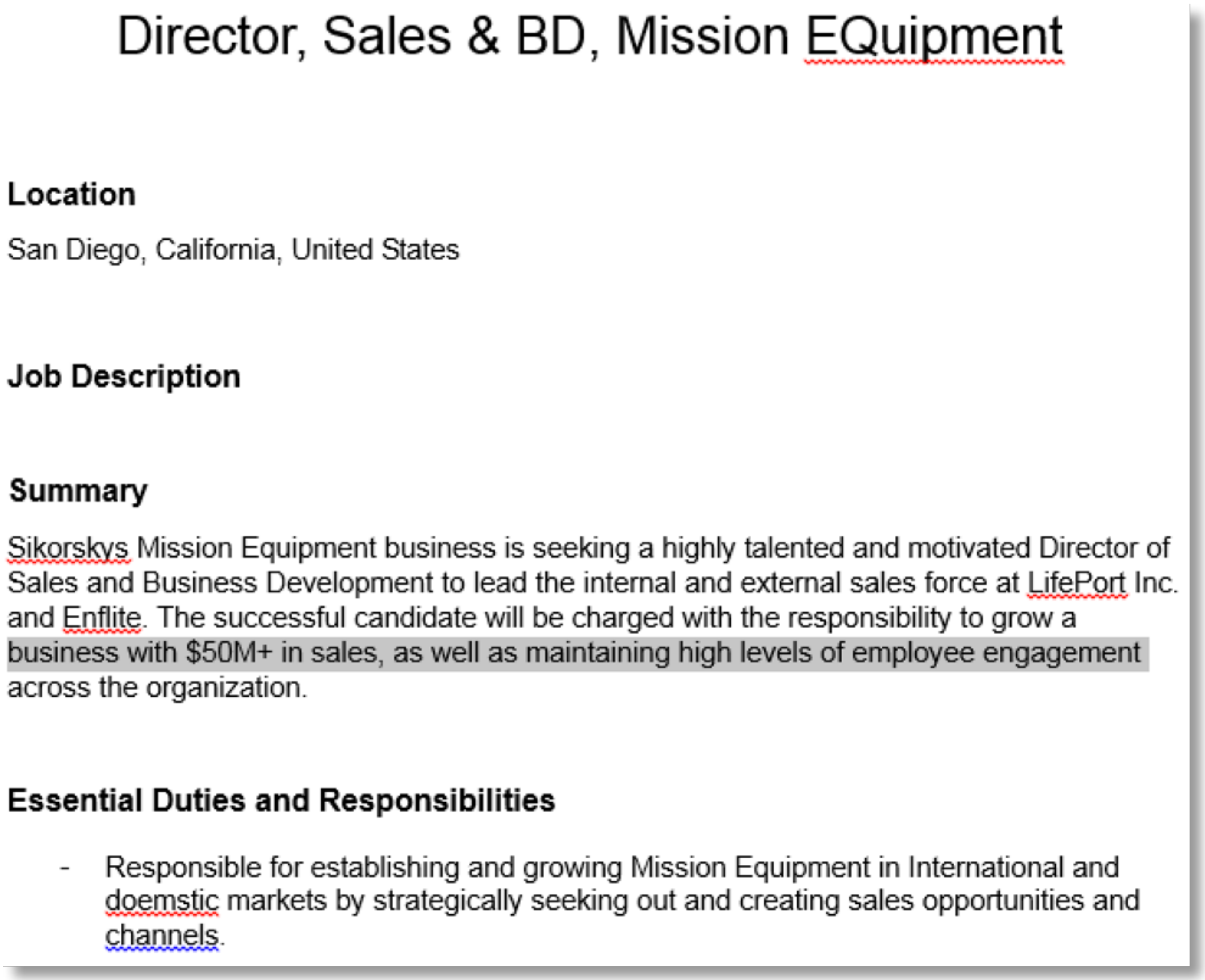
Primary duties include:

- Lead team in resolution of mechanical product test failures. Work closely with manufacturing facilities (LM and subcontractors) in the triage of test failures and planning and execution of root cause investigations and corrective action implementation. Be closely tied into tactics and report out status daily to executive leadership.
- Identify, plan and execute producibility improvements
- Manage professional engineering staff, establishing and maintaining appropriate headcount and salary grade mix; respond and adjust rapidly and urgently to emerging issues and apply resources appropriately; manage competing priorities and satisfy all schedule demands while adopting a fixed-price mentality
- Interface with Senior Manager and Director level leaders on Program and with MDA customers.
- Actively collaborate with the LOB and Engineering on critical needs and issues throughout the program

Basic Qualifications

- Minimum 8 years of technical experience with demonstrated expertise in complex missile, space, or aircraft systems.
- Experience leading technical teams
- Demonstrated technical depth and breadth in Mechanical Engineering, particularly in structures and/or propulsion/ordnance design and associated test equipment
- Excellent communication skills, both verbal and written, with the ability to articulate complex technical and programmatic issues to subordinates, peers, management and customers.
- Proven ability to drive closure and resolve technical issues/challenges
- Experience as Certified Principal Engineer (CPE) or equivalent design cognizant engineering role for missile, spacecraft or aircraft

The following images also shows the contents of a recent decoy document (062aadf3eb69686f4881860d88ce472e6b1c07e1f586d840dd2ee1f7b76cabe7). It contains an exact copy of a publicly available job description, including typos, at a US defense contractor.



Director, Sales & BD, Mission EQuipment

Location

San Diego, California, United States

Job Description

Summary

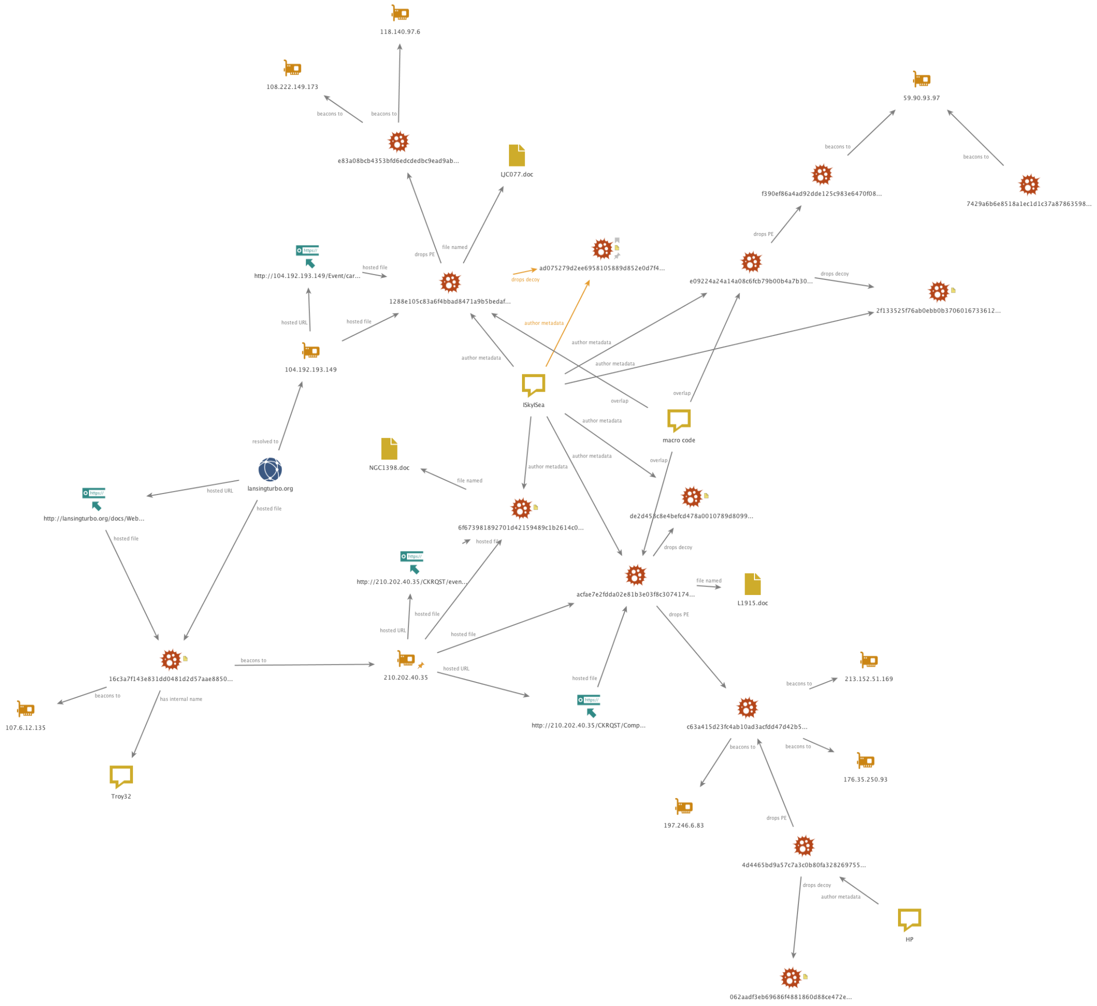
Sikorskys Mission Equipment business is seeking a highly talented and motivated Director of Sales and Business Development to lead the internal and external sales force at LifePort Inc. and Enflite. The successful candidate will be charged with the responsibility to grow a business with $50M+ in sales, as well as maintaining high levels of employee engagement across the organization.

Essential Duties and Responsibilities

- Responsible for establishing and growing Mission Equipment in International and doemstic markets by strategically seeking out and creating sales opportunities and channels.

The weaponized documents have been hosted on systems which we believe have likely been compromised and repurposed. Two of the URL paths used to host the weaponized documents on the compromised systems are exact matches (event/careers/jobs/description/docs). The payloads delivered by the weaponized documents are extremely similar to the payloads delivered by weaponized documents detailed in our April 2017 report on the threat group's activity.

For a more comprehensive understanding of the relationships between samples and infrastructure used in the recent activity see the following network graph.



The document metadata Author "ISkyISea" is used across multiple weaponized document files. IPv4 addresses (210.202.40[.]35) hosting the weaponized documents have also been hardcoded as command and control servers for previous samples (16c3a7f143e831dd0481d2d57aae885090e22ec55cc8282009f641755d423fcd).

Ties to Blockbuster

The source code used in the macros embedded in the weaponized documents described above was also detailed in a previous report where it was included in testing documents uploaded to VirusTotal. This reuse of macro source code, XOR keys used within the macro to decode implant payloads, and the functional overlap in the payloads the macros write to disk demonstrates the continued use of this tool set by this threat group. The use of an automated tool to build the weaponized documents would explain the common but not consistent reuse of metadata, payloads, and XOR keys within the documents.

Other similarities between the previously reported activity and this new activity can be seen within the PE payloads written to disk by the malicious documents. The payloads function similarly to other implants associated with this threat group. The use of a fake TLS communications protocol, encoded strings within samples, filenames and contents of batch files embedded within implants, as well implants beaconing directly to IPv4 addresses (and not resolving domains for command and control) are all known techniques associated with the threat group. These tactics have changed very little since the original Operation Blockbuster.

In addition to tool reuse, infrastructure overlaps also exist. URLs used for hosting the malicious documents and IPv4 addresses used for command and control overlap with infrastructure previously used by the group.

Final Thoughts

The techniques and tactics the group uses have changed little in recent attacks. Tool and infrastructure overlaps with previous campaigns are apparent. Given that the threat actors have continued operations despite their discovery and public exposure it is likely they will continue to operate and launch targeted campaigns.

Palo Alto Networks researchers will continue to monitor this group's activities and stay abreast to additional attacks using this tool set.

- The malicious files describe in this report are flagged as malicious by WildFire and in Threat Prevention.
- AutoFocus users can learn more about the threat group and their indicators by examining the BlockBuster_Sequel tag.

Indicators of Compromise

SHA256

4d4465bd9a57c7a3c0b80fa3282697554a1419794afa36e544a4ae06d60c1615

f390ef86a4ad92dde125c983e6470f08344b9eaa14c17a1e6c4bb7ebfa7c4ec9

acfae7e2fdda02e81b3e03f8c30741744d629cd672db424027f7caa59c975897

7429a6b6e8518a1ec1d1c37a8786359885f2fd4abde560adaef331ca9deaeefd

e09224a24a14a08c6fcb79b00b4a7b3097c84f805f5f2adefe2f7d04d7b4a8ee

062aadf3eb69686f4881860d88ce472e6b1c07e1f586d840dd2ee1f7b76cabe7

c63a415d23fc4ab10ad3acfdd47d42b5c7444604485ab45147277cca82fffb34

16c3a7f143e831dd0481d2d57aae885090e22ec55cc8282009f641755d423fcd

de2d458c8e4befcd478a0010789d80997793790b18a347d10a595d6e87d91f34

2f133525f76ab0ebb0b370601673361253074c337f0b0895d0f0cb5bc261cfcb e83a08bcb4353bfd6edcdedbc9ead9ab179a620e15155b60d18153bed9892f38

6f673981892701d42159489c1b2614c098a04e4674b23e1cd0fd8911766e71a0

ad075279d2ee6958105889d852e0d7f4266f746cb0078ac1b362f05a45b5828d

1288e105c83a6f4bbad8471a9b5bedafeea684a8d8b73a1a7518137d446c2e1e

IPv4

104.192.193[.]149

176.35.250[.]93

213.152.51[.]169

108.222.149[.]173

197.246.6[.]83

118.140.97[.]6

210.202.40[.]35

59.90.93[.]97

107.6.12[.]135

URLs

http://210.202.40[.]35/CKRQST/event/careers/jobs/description/docs/NGC1398.doc

http://210.202.40[.]35/CKRQST/Company/HR/Position/lm/L1915.doc

http://104.192.193[.]149/Event/careers/jobs/description/docs/LJC077.doc

http://lansingturbo[.]org/docs/WebDAV.exe