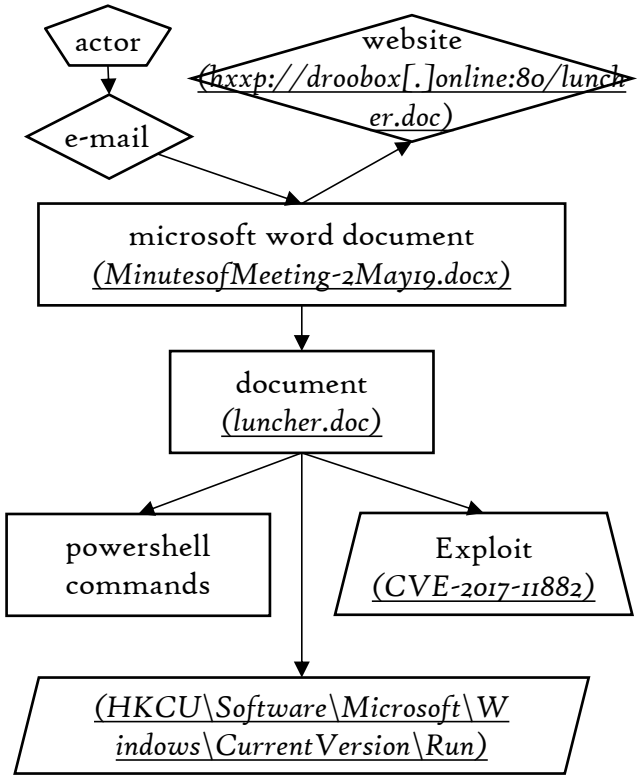
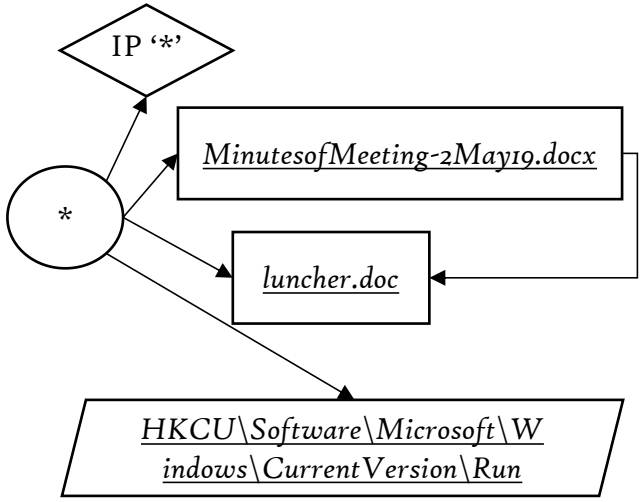
https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

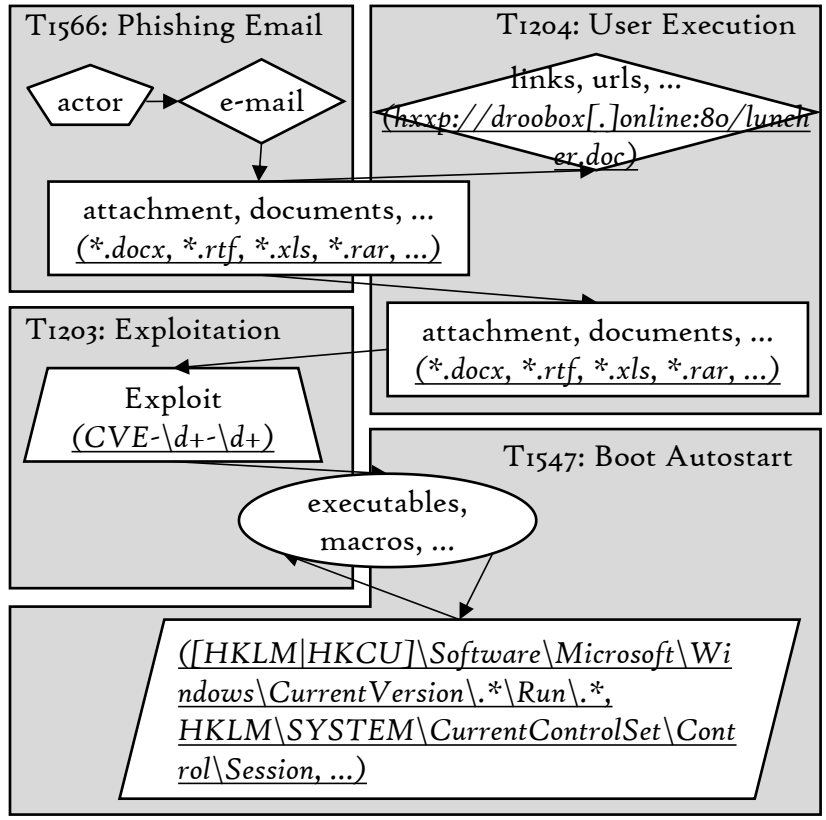
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named MinutesofMeeting-2May19.docx. Once the victim opens the document, it fetches a remove template from the actor-controlled website, hxxp://droobox[.]online:80/luncher.doc. Once the luncher.doc was downloaded, it used CVE-2017-11882, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run Registry key.



(A) Manually generated attack graph



(D) Attack graph by "EXTRACTOR"



(E) Knowledge-enhanced attack graph

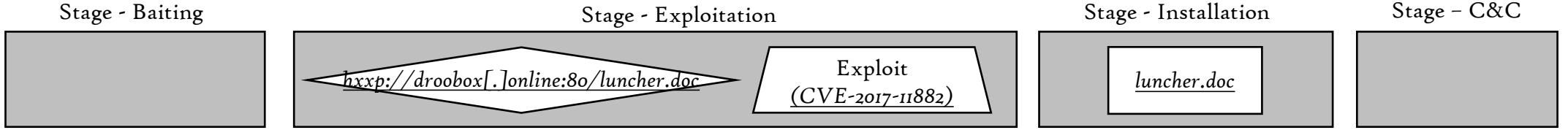
(FP) T1048: Exfiltration Over Alternative Protocol | T1203: Exploitation | T1547: Boot Autostart

Sent: microsoft word document (MinutesofMeeting-2May19.docx)

Use: Exploit (CVE-2017-11882)

Adding to: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

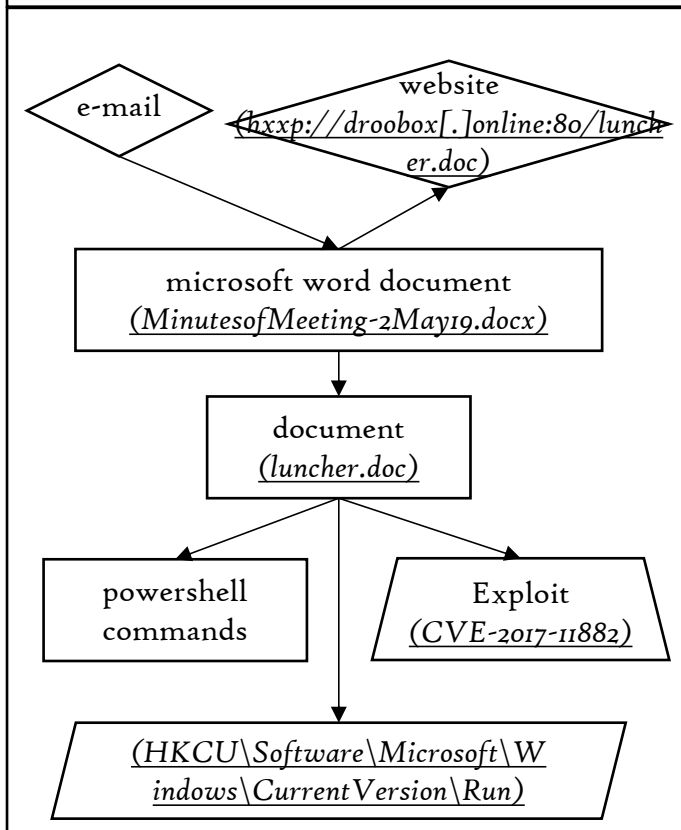
(B) Part of attack techniques extracted with "TTPDrill"



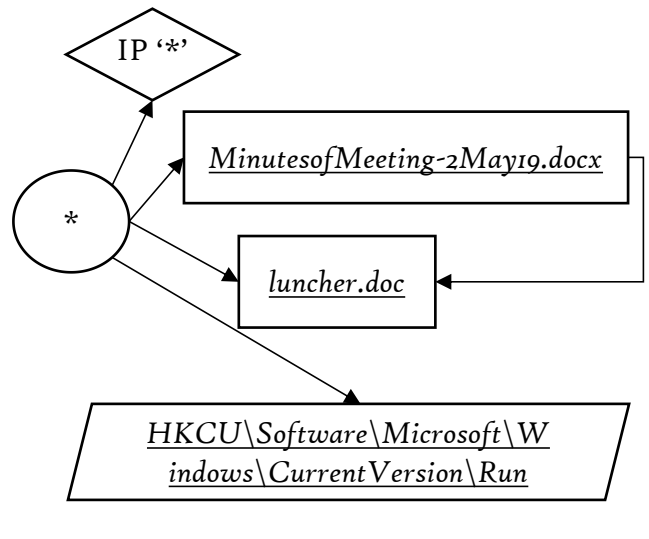
(C) Attack chain extracted with "ChainSmith"

https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

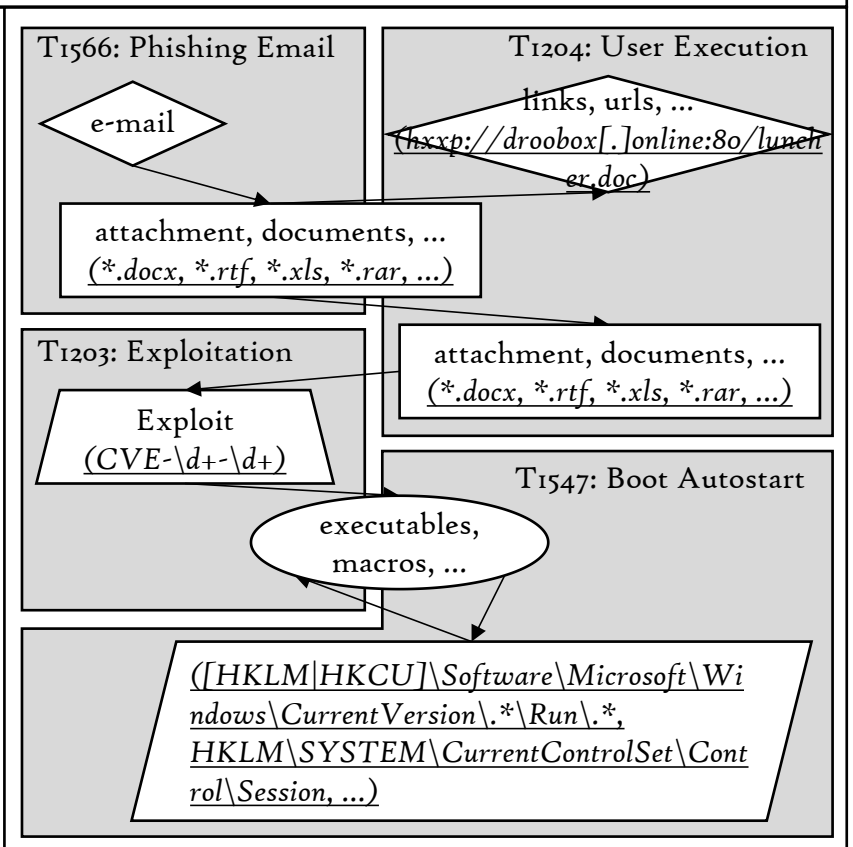
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named MinutesofMeeting-2May19.docx. Once the victim opens the document, it fetches a remove template from the actor-controlled website, hxxp://droobox[.]online:80/luncher.doc. Once the luncher.doc was downloaded, it used CVE-2017-11882, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run Registry key.



(A) Manually generated ground-truth

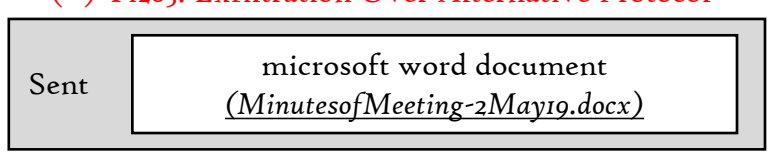


(D) Attack graph generated by "EXTRACTOR"

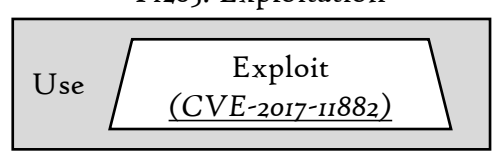


(E) Attack technique graph generated by us

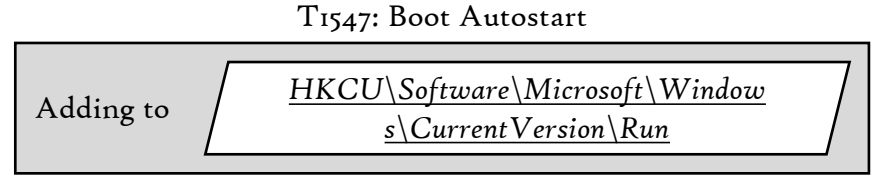
(×) T1203: Exfiltration Over Alternative Protocol



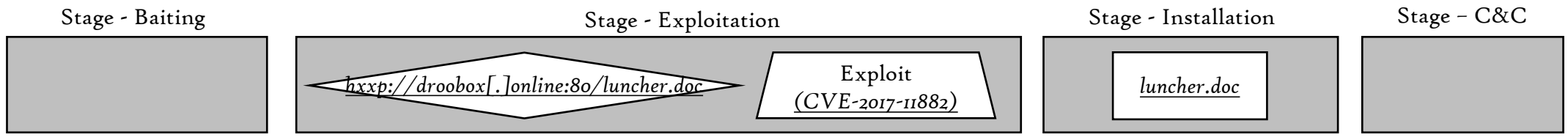
T1203: Exploitation



T1547: Boot Autostart

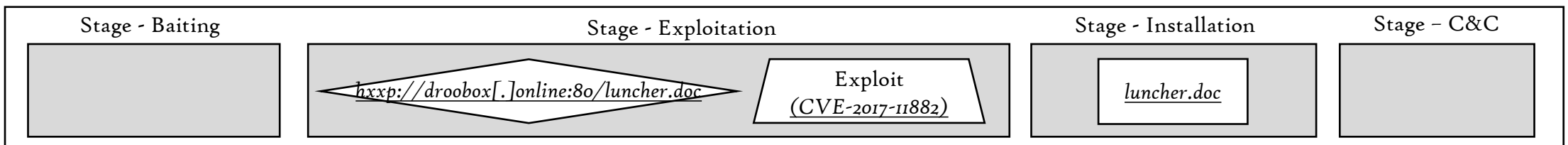


(B) Attack techniques extracted with "TTPDrill"

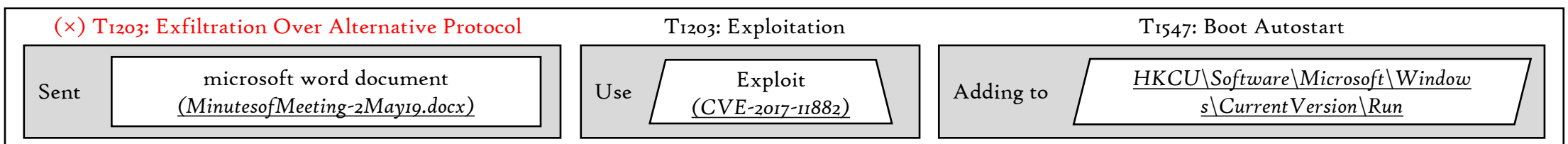


(C) Attack chain extracted with "ChainSmith"

The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named *MinutesofMeeting-2May19.docx*. Once the victim opens the document, it fetches a remove template from the actor-controlled website, *hxxp://droobox[.]online:80/luncher.doc*. Once the *luncher.doc* was downloaded, it used *CVE-2017-11882*, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* Registry key.



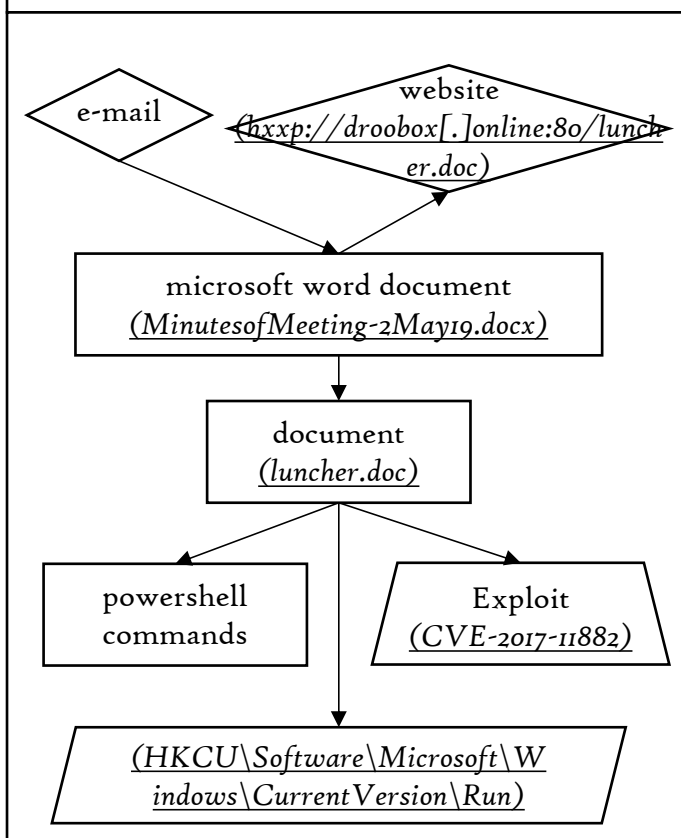
(C) Attack chain extracted with "ChainSmith"



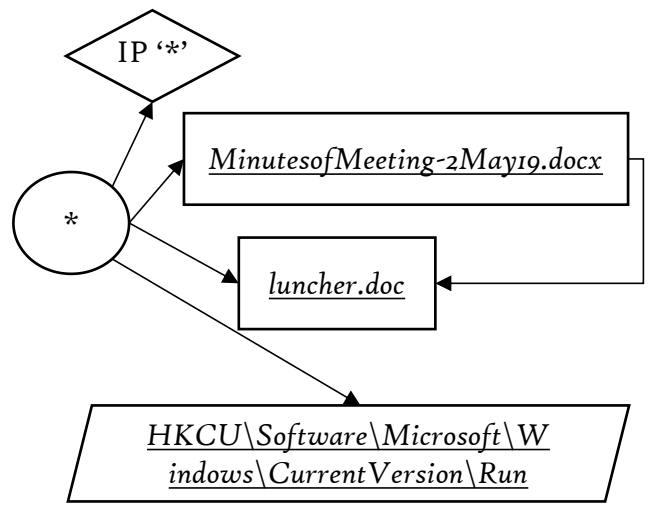
(B) Attack techniques extracted with "TTPDrill"

https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

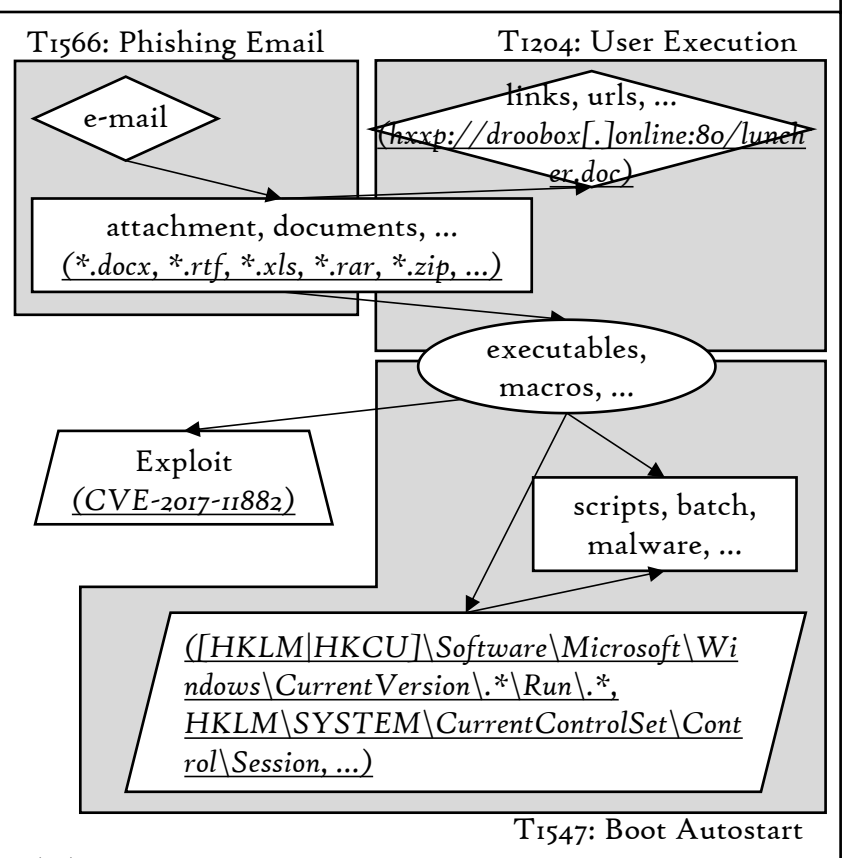
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named *MinutesofMeeting-2May19.docx*. Once the victim opens the document, it fetches a remove template from the actor-controlled website, *hxxp://droobox[.]online:80/luncher.doc*. Once the *luncher.doc* was downloaded, it used *CVE-2017-11882*, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* Registry key.



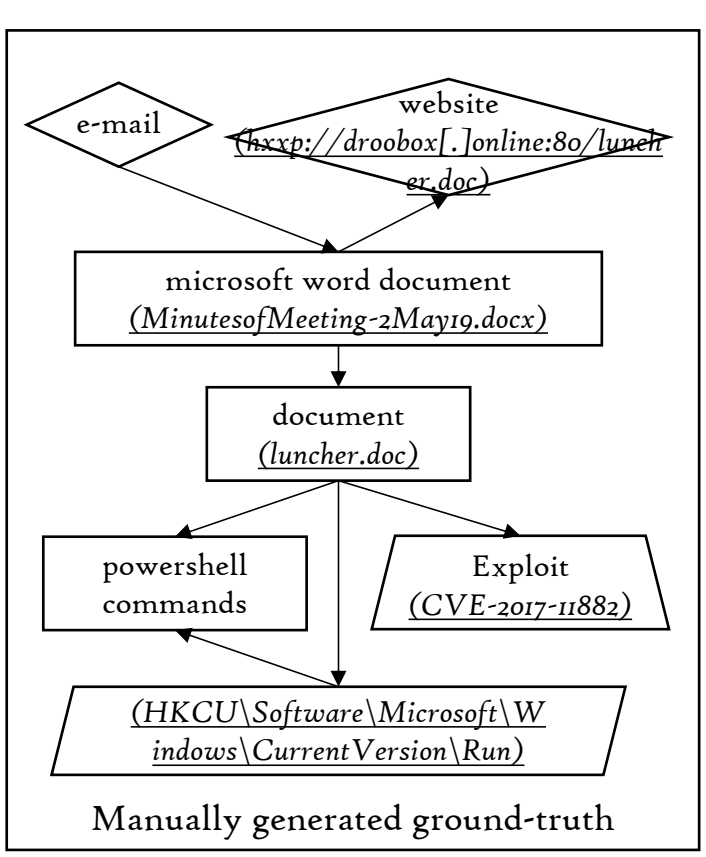
(A) Manually generated ground-truth



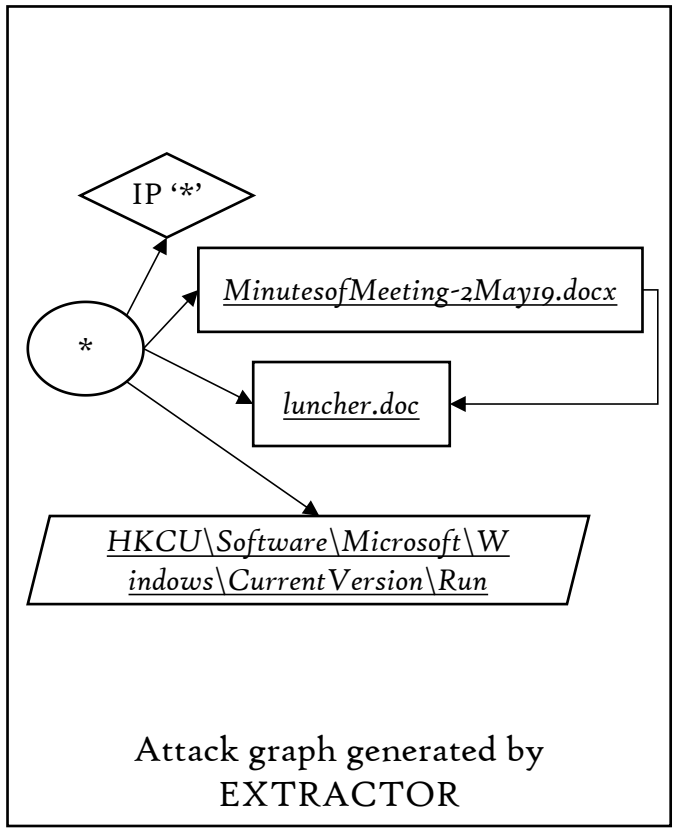
(B) Attack graph generated by "EXTRACTOR"



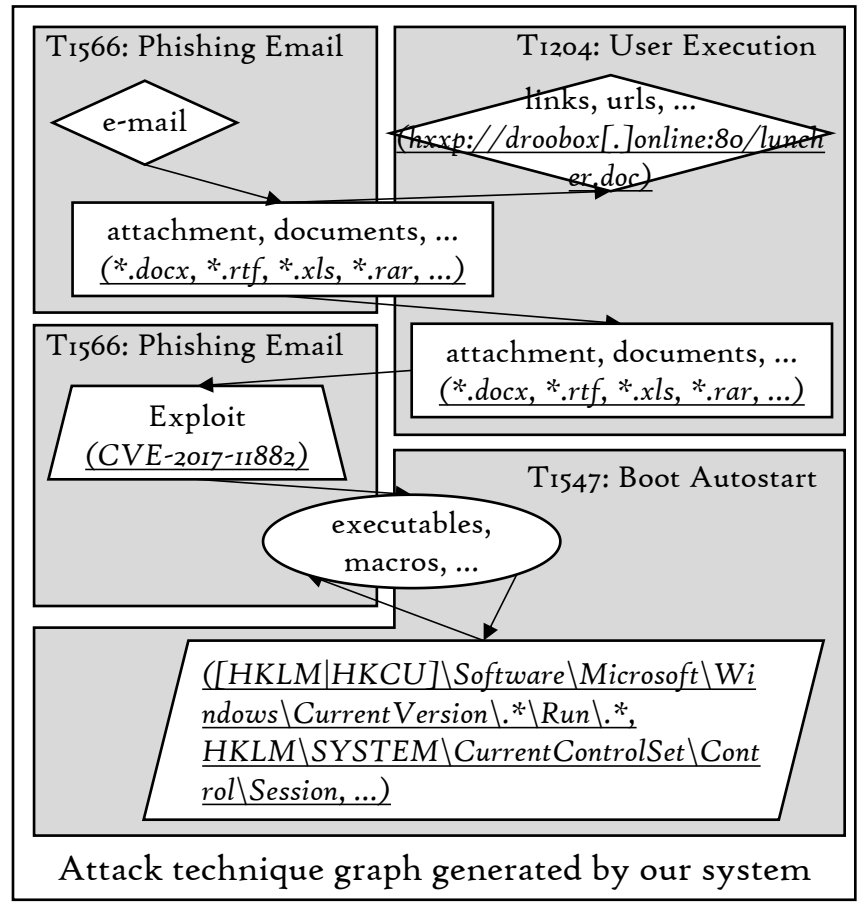
(C) Attack technique graph generated by AttackG



Manually generated ground-truth



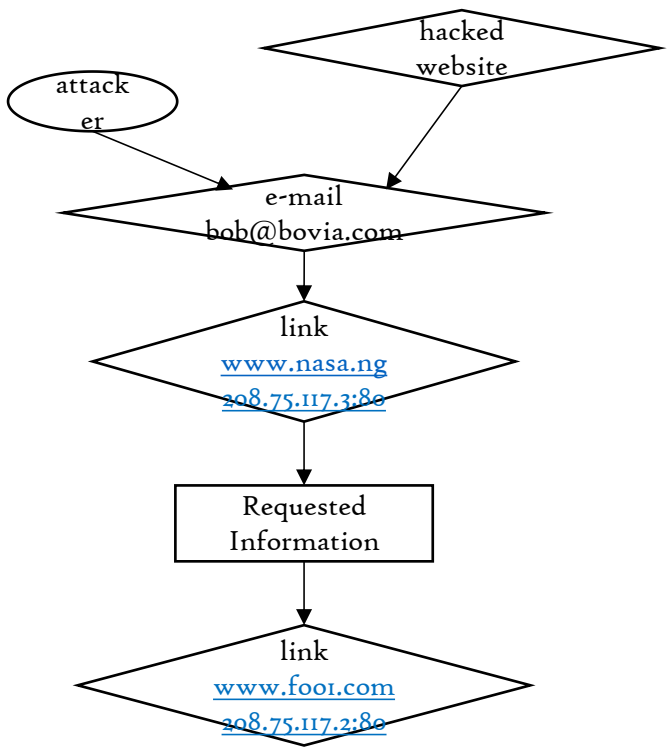
Attack graph generated by EXTRACTOR

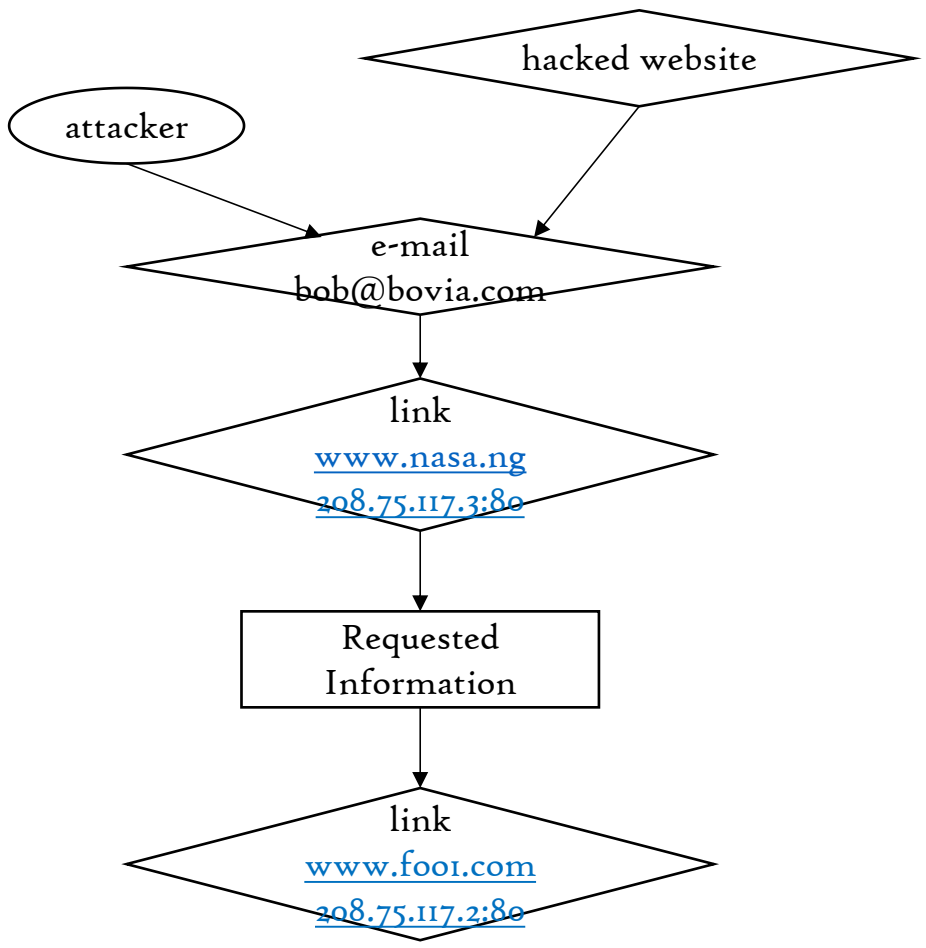


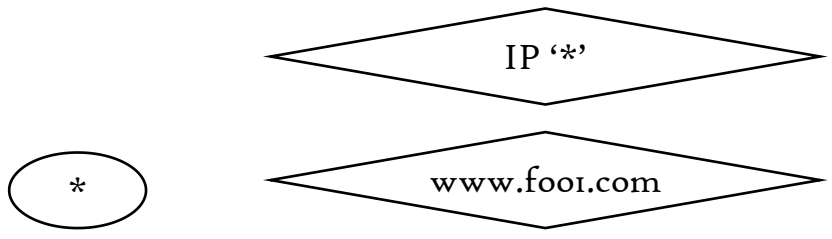
Attack technique graph generated by our system

20180410 1200 TRACE – Phishing E-mail Link

The attacker ran an attack against ClearScope. The attacker found the e-mail address of the phone user, bob@bovia.com, previously from a data dump from a hacked website. The attacker sent a phishing e-mail to Bob impersonating the Bovia Company Benefits Open Enrollment group. The phishing e-mail included a link to a website hosted at www.nasa.ng, address 208.75.117.3:80. The website hosted a form asking for name, e-mail address, and password. The user unfortunately clicked on the link, entered the requested information, and submitted it. The results were sent back to www.foo1.com, address 208.75.117.2:80. The attacker now has access to Bob's e-mail account, including contact information for other Bovia company employees.




hacked website
attacker
e-mail
bob@bovia.com
link
www.nasa.ng
208.75.117.3:80
Requested
Information
link
www.foo1.com
208.75.117.2:80


IP '*'
*
www.foo1.com