Digital Quartermaster Scenario Demonstrated in Attacks Against the Mongolian Government

researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

Josh Grunzweig, Robert Falcone, Bryan Lee March 14, 2016

By Josh Grunzweig, Robert Falcone and Bryan Lee

March 14, 2016 at 1:00 PM

Category: Government, Threat Prevention, Unit 42

Tags: BBSRAT, cmstar, Digital Quartermaster, Mongolia

This post is also available in: 日本語 (Japanese)

Unit 42 has collected multiple spear phishing emails, weaponized document files, and payloads that targeted various offices of the Mongolian government during the time period of August 2015 and February 2016. The phishing emails and document files leveraged a variety of geopolitically sensitive subject matters as attractive lures, such as events in Beijing, the Dalai Lama, North Korea relations, the Zika virus, and various legitimate appearing announcements. As we began to analyze and tear down the various samples we collected, we found significant overlaps with previously reported and documented adversary groups, attack campaigns, and their toolsets, exemplifying the concept of the Digital Quartermaster.

The concept of the Digital Quartermaster is not a particularly new one; it is the idea that there is a group, or groups whose mission is to supply and maintain malicious tools in support of cyber espionage operations. The existence of a Digital Quartermaster has been discussed within the intelligence community for some time, but it is not often that sufficient overlaps exist between what appear to be separate toolsets to confidently claim this idea is indeed in use. The data Unit 42 has collected and analyzed however, does strongly point to the possibility that while there may be multiple operations groups, a Digital Quartermaster may be the one supplying and maintaining the tools used.

Attack Analysis

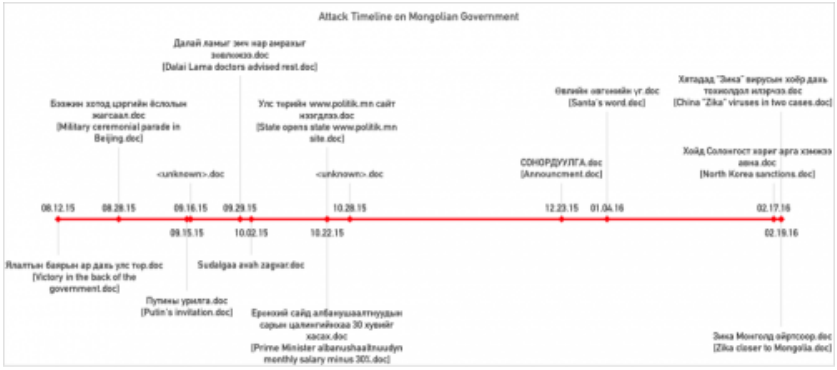
While investigating new BBSRAT instances discovered using the AutoFocus tool, Unit 42 was able to collect additional samples, weaponized documents, and phishing emails uploaded to VirusTotal between August 2015 through February 2016. Each of the samples collected via WildFire and VirusTotal contained significant overlaps in tactics used, tools used, as well as infrastructure for command and control channels. In addition, a large majority of the samples gathered from VirusTotal were uploaded from a single entity in Mongolia.

The attacks themselves followed a consistent playbook throughout the observed timeframe; using weaponized Microsoft Word documents initially containing an exploit for only CVE-2012-0158, appearing to use the highly popular ‘Tran Duy Linh’ toolkit, then adding in an additional exploit for CVE-2014-1761 in the three newest samples we collected. The newer documents containing exploits for both vulnerabilities appeared to use a publically available PoC authored by ‘HCL’, with little to no modifications made. All of the weaponized documents except two executed the Cmstar loader or a lightly modified variant of Cmstar onto the victim host while displaying a decoy document or a legitimate appearing document that is generated and presented to the user to make it appear that the weaponized document that had been executed was indeed, legitimate. Once Cmstar was loaded onto the victim hosts, it would attempt to retrieve a final payload. Unfortunately, at the time of analysis, we

were unable to retrieve the majority of the payloads the Cmstar loaders were attempting to download, but those that were available were variants of BBSRAT. The two samples not using Cmstar simply had BBSRAT embedded directly into to the weaponized document.

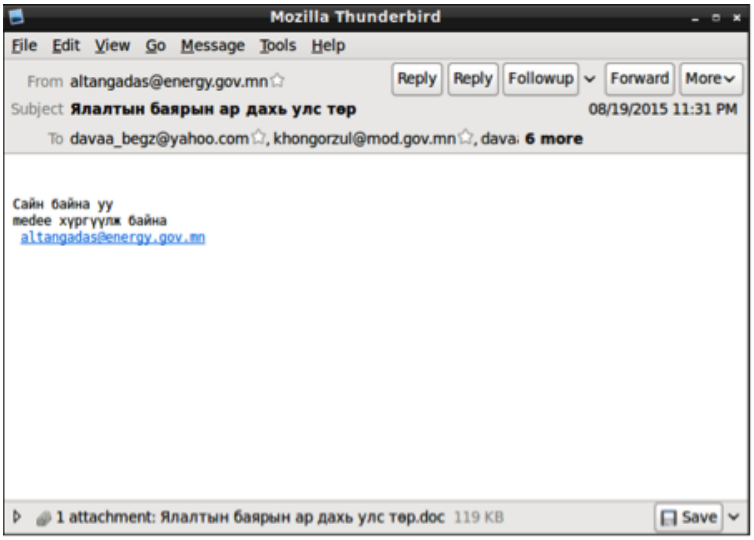
Furthermore, examining the data from August indicates that this campaign had started earlier and the adversary may have already achieved initial footholds, due to the use of what appears to be compromised legitimate email accounts from within the Mongolian government.

Attack Timeline



Attack Details

SHA256	5beb50d95c1e720143ca0004f5172cb8881d75f6c9f434ceaff59f34fa1fe378
Date	8/12/2015
Filename	Ялалтын баярын ар дахь улс төр.doc (Victory in the back of the government)
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Two spear-phishing emails originating from likely compromised account 'altangadas@energy.gov.mn' targets multiple other Mongolian government officials. The subject and file attachment are titled 'Ялалтын баярын ар дахь улс төр' (Victory in the back of the government). CVE-2012-0158 exploit used, dropping new variant of Cmstar. The dropped decoy document talks about a Russian festival known as 'Victory Day' and Mongolian's participation in this event.



Ялалтын баярын ар дахь улс төр

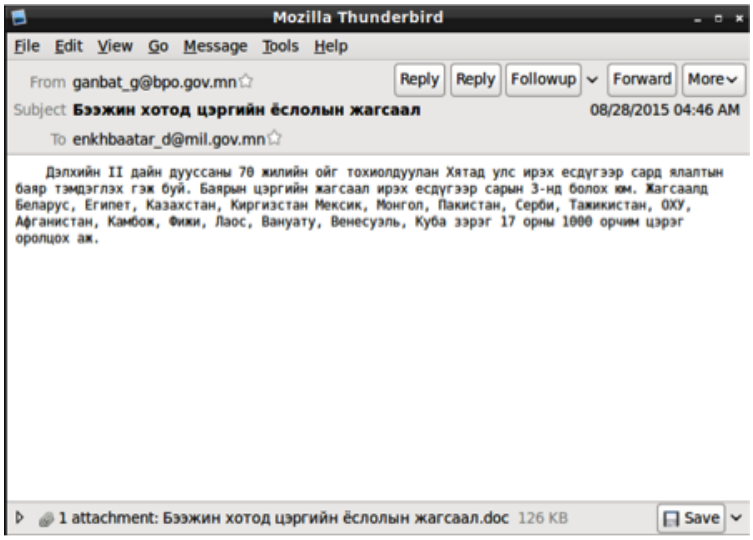
Маргааш манай хойд хөрш ОХУ-ын нийслэл хотноо оросын ард түмэнд Гитлерийн Германы армийг бут цохисоны 70 жилийн ой ёслол төгөлдөр тэмдэглэх гэж байна. Оросууд энэ баярыг Аугаа их эх орны дайны ялалтын баярын өдөр гэж нэрлэдэг. Ялалтын баярыг тэмдэглэж ирсэн 1945 оноос хойш хамгийн их буюу 16 мянга гаруй цэргийн албан хаагч маргаашийн баярын парадад оролцоно. Мөн хуурай замын цэргийн 194 техник, 143 онгоц нисдэг тэрэг оролцоно. Гитлерийн Германыг бут цохиход оросын ард түмэнтэй мөр зэрэгцэн тулалдаж явсан арав гаруй орны цэргийн төлөөлөл Улаан талбайд хөл тавихын нэг нь Монгол цэргүүд байх юм. ОХУ-ын удирдагчид энэ баяраар цэргийн шинэ зэвсэглэлүүдээ олны өмнө ил гаргах гэж байна. Парадын бэлтгэлийг Москва хотноо шөнийн цагаар хийж байгаа бөгөөд энэ долоо хоногоос хөл тавих цэргийн жагсаалаас гадна цэргийн хүнд техникүүдийн үзүүлбэрийг сургуулилж эхэлжээ. Тавдугаар сарын 9-ний баярын жагсаалыг яг давтан бэлтгэж байгаа учраас "жинхэнэ" парадыг телевизээр биш "амьдаар" нь харах гэсэн москвачууд Улаан талбайд ихээр цугларч байгаа аж. Оросын цэргийн сүүлийн танк болох "Армата" олны анхаарлыг ихээр татаад байгаа бөгөөд харсан хүн бүр "үнэхээр сайхан амьтан юм" хэмээн шүүрс алдаж байгаа талаар Оросын хэвлэлүүд бичиж байна.

Крым болон Украины хэрэг явдлаас хойш ОХУ-ын баруун зүг дэх харилцаа холбоо хүйтэрч, улс төрийн болоод эдийн засгийн хувьд зүүн зүг рүү харилцаа зузаатгахаар зорьж байгаа. Энэ зүгт ОХУ-ын хамгийн том түнш бол Хятад. Өнгөрсөн жилээс ОХУ-ЫНХАУ-ын хооронд эдийн засгийн том том төслүүдийг хэрэгжүүлэх гэрээнүүдийг зурж, хэрэгжүүлэх шатандаа явж байгаа.

Путин уг нь энэ ялалтын баярыг Сочигийн өвлийн олимпийн тоглолтын нэгэн адил агуу Орос орны сүр хүчийг харуулах нэгэн боломж болгохоор зорьсон ч хүссэнээр нь болохгүй нь. Дэлхийн олон орны төрийн тэргүүн нарт ялалтын баярт оролцох урилгыг өнгөрсөн жил илгээсэн ч эцсийн мөчид гуч хүрэхгүй орны төрийн тэргүүн маргааш Улаан талбайд ялалтын парад үзнэ. АНУ болон Европын холбооны орнуудын ихэнх нь Кремлийн урилгаас эелдэгхэн татгалзсан ч үнэн хэрэгтээ Крым болон Украины асуудлаар ОХУ-ын барьж байгаа байр суурийг эсэргүүцсэн нь тодорхой. Тавдугаар сарын 9-нд Улаан талбайд хэн хэн очих талаар гадаадын хэвлэлүүд ихээхэн бичиж, анхаарал хандуулсан. Кремлийн зүгээс ч энэ асуултад хариулахад төвөгтэй байсан нь тодорхой. Ямар сайндаа л өнгөрсөн Мягмар гаригт ОХУ-ын Гадаад хэргийн сайд Сергей Лавров Австрийн Гадаад хэргийн сайдтай хамт хийсэн хэвлэлийн бага хурлын үеэр "Энэ бол бидний баяр. Урилга бол цэргийн зарлан дуудах хуудас биш, хэрвээ хэн нэг нь бидний урилгыг хүлээн авах боломжгүй бол бид үүнийг ойлгож байна" хэмээн мэдэгдэж байхав. Хойд Солонгосын залуу удирдагч Ким Чен Ун-ыг Улаан талбайд зогсох хамгийн содон зочин байна гэж тооцоолж байсан ч эцсийн мөчид очих боломжгүй гэдгээ мэдэгдсэн. Манай урд хөрш БНХАУ-ын дарга Си Жиньпин ялалтын баярт оролцохоор өчигдөр Бээжингээс мордсон байна. Тэрбээр ялалтын баярт оролцохоос гадна залгуулаад Казахстан, Беларусьт айлчлах юм. Ялалтын баярт оролцохоор Монгол Улсын Ерөнхийлөгч Ц.Элбэгдорж өнгөрсөн Лхагва гаригт Москвад очсон билээ.

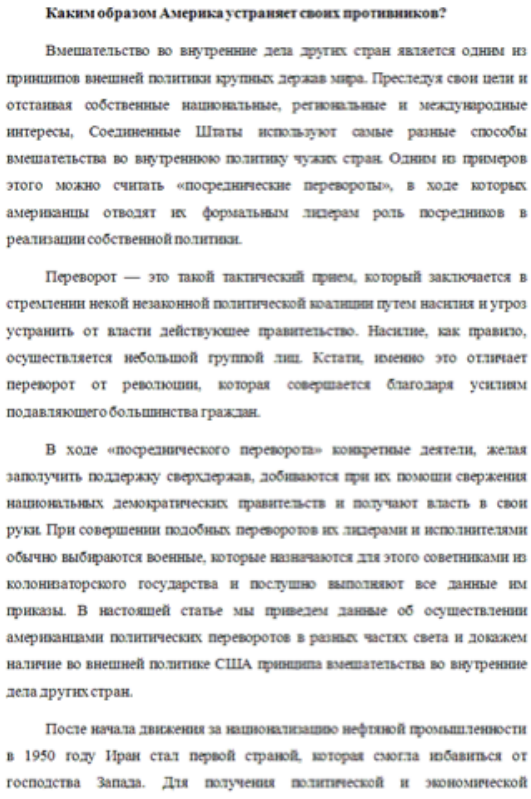
Үнэндээ хэн урилгыг хүлээн авч, хэн урилгаас татгалзав гэдгээр дэлхийд үүсээд

SHA256	10090692ff40758a08bd66f806e0f2c831b4b9742bbf3d19c250e778de638f57
Date	8/28/2015
Filename	Бээжин хотод цэргийн ёслолын жагсаал.doc (Military ceremonial parade in Beijing)
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Spear-phishing email originating from 'ganbat_g@bpo.gov.mn'. A single target is discovered in the collected sample. Subject and filename are titled 'Бээжин хотод цэргийн ёслолын жагсаал' (Military ceremonial parade in Beijing). CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy document contains a flight itinerary from Ulaanbaatar, Mongolia to Beijing, China.



SHA256	44dbf05bc81d17542a656525772e0f0973b603704f213278036d8ffc999bb79a
Date	9/15/2015
Filename	Путины урилга.doc (Putin's Invitation)
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Weaponized Microsoft Word document found titled 'Путины урилга.doc' (Putin's Invitation). CVE-2012-0158 exploit used, dropping new variant of Cmstar. The following decoy image, embedded within a Word document, is displayed to the victim upon opening the malicious file.

SHA256	91ffe6fab7b33ff47b184b59356408951176c670cad3afcde79aa8464374acd3
Date	9/16/2015
Filename	1.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Weaponized Microsoft Word document with unknown title found. Likely delivered via spear-phishing. CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy document, which is 13 pages in length, talks about the interference of the United States in other countries across the globe.



Каким образом Америка устраняет своих противников?

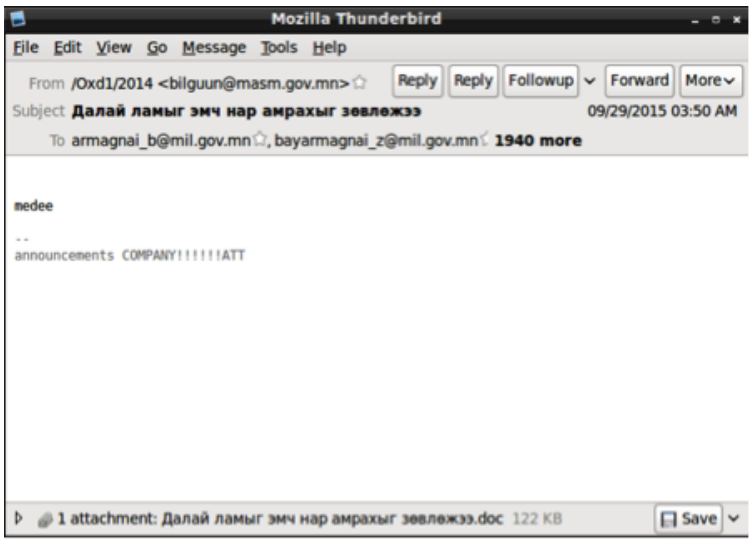
Вмешательство во внутренние дела других стран является одним из принципов внешней политики крупных держав мира. Преследуя свои цели и отстаивая собственные национальные, региональные и международные интересы, Соединенные Штаты используют самые разные способы вмешательства во внутреннюю политику чужих стран. Одним из примеров этого можно считать «посреднические перевороты», в ходе которых американцы отводят их формальным лидерам роль посредников в реализации собственной политики.

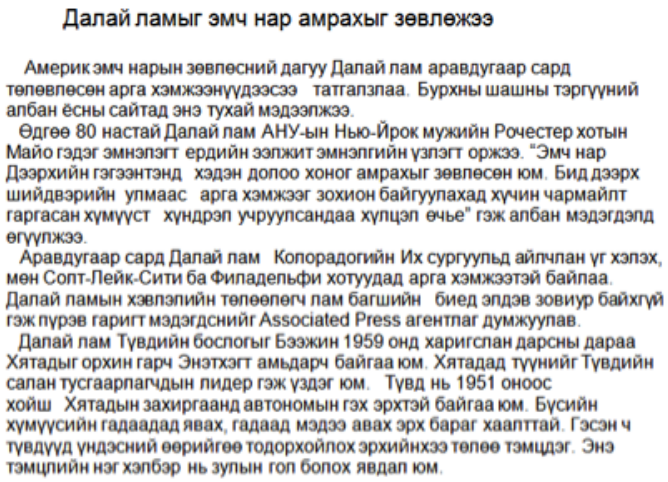
Переворот — это такой тактический прием, который заключается в стремлении некой незаконной политической коалиции путем насилия и угроз устранить от власти действующее правительство. Насилие, как правило, осуществляется небольшой группой лиц. Кстати, именно это отличает переворот от революции, которая совершается благодаря усилиям подавляющего большинства граждан.

В ходе «посреднического переворота» конкретные деятели, желая заполучить поддержку сверхдержав, добиваются при их помощи свержения национальных демократических правительств и получают власть в свои руки. При совершении подобных переворотов их лидерами и исполнителями обычно выбираются военные, которые назначаются для этого советниками из колонизаторского государства и послушно выполняют все данные им приказы. В настоящей статье мы приведем данные об осуществлении американцами политических переворотов в разных частях света и докажем наличие во внешней политике США принципа вмешательства во внутренние дела других стран.

После начала движения за национализацию нефтяной промышленности в 1950 году Иран стал первой страной, которая смогла избавиться от господства Запада. Для получения политической и экономической

SHA256	6f3d4fb64de9ae61776fd19a8eba3d1d828e7e26bb89ace00c7843a57c5f6e8a
Date	9/29/2015
Filename	Далай ламыг эмч нар амрахыг зөвлөжээ.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Spear-phishing email originating from 'bilguun@masm.gov.mn'. Nearly two thousand recipients found to be targeted, all within the Mongolian government. Email subject and filenames titled 'Далай ламыг эмч нар амрахыг зөвлөжээ' (Dalai Lama doctors advised rest). CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy document discusses the latest health of the Dalai Lama, as well as a number of US-based trips he made in late 2015.





Далай ламыг эмч нар амрахыг зөвлөжээ

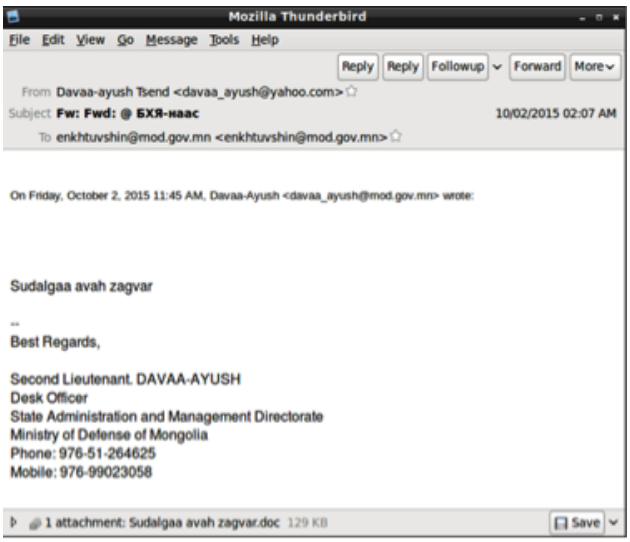
Америк эмч нарын зөвлөсний дагуу Далай лам аравдугаар сард төлөвлөсөн арга хэмжээнүүдээсээ татгалзлаа. Бурхны шашны тэргүүний албан ёсны сайтад энэ тухай мэдээлжээ.

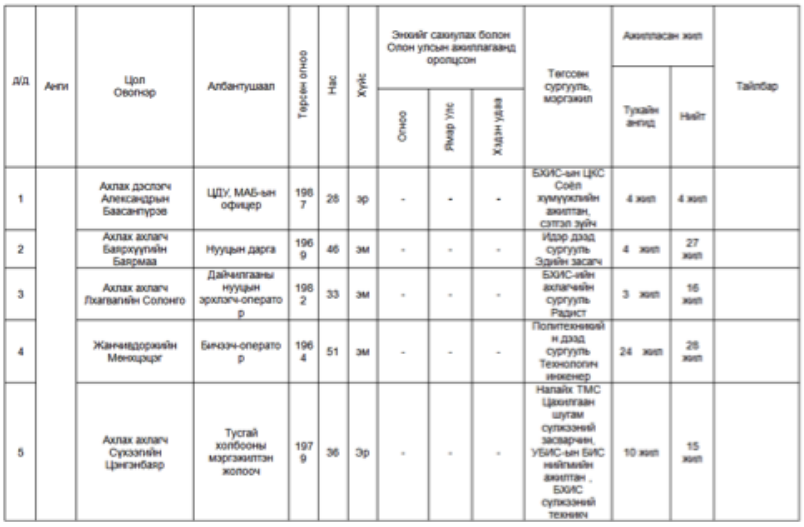
Өдгөө 80 настай Далай лам АНУ-ын Нью-Йорк мужийн Рочестер хотын Майо гэдэг эмнэлэгт ердийн эрлжит эмнэлгийн үзлэгт оржээ. "Эмч нар Дээрхийн гэгээнтэнд хэдэн долоо хоног амрахыг зөвлөсөн юм. Бид дээрх шийдвэрийн улмаас арга хэмжээг зохион байгуулахад хүчин чармайлт гаргасан хүмүүст хүндрэл учруулсандаа хүлцэл өчье" гэж албан мэдэгдэлд өгүүлжээ.

Аравдугаар сард Далай лам Колорадогийн Их сургуульд айлчлан үг хэлэх, мөн Солт-Лейк-Сити ба Филадельфи хотуудад арга хэмжээтэй байлаа. Далай ламын хэвлэлийн төлөөлөгч лам багшийн биед эрдэв зовиур байхгүй гэж нүрэв гаригт мэдэгдснийг Associated Press агентлаг думжуулав.

Далай лам Түвдийн бослогыг Бээжин 1959 онд харигслан дарсны дараа Хятадыг орхин гарч Энэтхэгт амьдарч байгаа юм. Хятадад түүнийг Түвдийн салан тусгаарлагчдын лидер гэж үздэг юм. Түвд нь 1951 оноос хойш Хятадын захиргаанд автономын гэх эрхтэй байгаа юм. Бүсийн хүмүүсийн гадаадад явах, гадаад мэдээ авах эрх бараг хаалттай. Гэсэн ч түвдүүд үндэсний өөрийгөө тодорхойлох эрхийнхээ төлөө тэмцдэг. Энэ тэмцлийн нэг хэлбэр нь зулын гол болох явдал юм.

SHA256	e88ea5eb642eaf832f8399d0337ba9eb1563862ddee68c26a74409a7384b9bb9
Date	10/2/2015
Filename	Sudalgaa avah zagvar.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Spear-phishing email originating from 'davaa_ayush@yahoo.com'. 'davaa_ayush@mod.gov.mn' was a target in the August 12, 2015 attack, indicating the user may have had their personal email account compromised as well. Single target found. Email subject is 'Fw:_Fwd:_@_БХЯ-наас' (Defense Ministry). Filename is titled 'Sudalgaa avah zagvar.doc', a possible Romanization of Mongolian. CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy table provides information about the rank, class, date of birth, and experience of individuals in the Mongolian armed forces.





д/д	Анги	Цол Овогнэр	Албантушаал	Төрсөн огноо	Нас	Хүйс	Энхийг сахиулах болон Олон улсын ажиллагаанд оролцсон			Төгссөн сургууль, мэргэжил	Ажилласан жил		Тайлбар
							Огноо	Ямар улс	Хэдэн удаа		Тухайн анхид	Нийт	
1		Ахлах дэслэгч Александрын Баасантуров	ЦДУ, МАБ-ын офицер	1987	28	эр	-	-	-	БХИС-ын ЦКС Соёл хүмүүжлийн ажилтан, сэтгэл зүйч	4 жил	4 жил	
2		Ахлах ахлагч Баярхүүгийн Баярмаа	Нууцын дарга	1969	46	эм	-	-	-	Идэр дээд сургууль Эдийн засагч	4 жил	27 жил	
3		Ахлах ахлагч Лхагвагийн Солонго	Дайчилгааны нууцын эрхлэгч-оператор	1982	33	эм	-	-	-	БХИС-ийн ахлагчийн сургууль Радист	3 жил	16 жил	
4		Жанчивдоржийн Менхцэцэг	Бичээч-оператор	1964	51	эм	-	-	-	Политехникийн дээд сургууль Технологич инженер	24 жил	28 жил	
5		Ахлах ахлагч Сүхээгийн Цэнгэнбаяр	Тусгай холбооны мэргэжилтэн жолооч	1979	36	Эр	-	-	-	Нарийн ТМС Цэхэлгэн шугам сүлжээний засварчин, УБИС-ын БИС нийлмэйн ажилтан , БХИС сүлжээний техникч	10 жил	15 жил	

ЗӨВСӨГТ ХҮЧНИЙ ... ДУГААР АНГИУДЫН ЦДУ-ЫН ОФИЦЕР, МАБ-ЫН ОФИЦЕР, НУУЦЫН ДАРГА НАРТ

Жич: Судалгааг үнэн зөв бөглөх ёстой анхааруулж байна.

СУДАЛГАА ГАРГАСАН:
... албан тушаал
... цол ... овог нэр

SHA256	68f97bf3d03b1733944c25ff4933e4e03d973ccdd73d9528f4d68806b826735e
Date	10/22/2015
Filename	албанушаалтнуудын сарын цалингийнхаа 30 хувийг хасах.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Weaponized Microsoft Word document found titled 'Ерөнхий сайд албанушаалтнуудын сарын цалингийнхаа 30 хувийг хасах.doc' (Prime Minister albanushaaltnuudyn monthly salary minus 30%.doc). Likely delivered via spear-phishing. CVE-2012-0158 exploit used, dropping new variant of Cmstar The document discusses changes made to the salaries of government officials within the Mongolian government

өндөр албанушаалтнуудын сарын цалингийнхаа 30 хувийг хасах

Өнөөдрийн байдлаар төсвийн орлого 600 гаруй тэрбумаар тасарсан, оны эцэс буюу ердөө хоёрхон сарын дараа энэ тоо нэг их наядад хүрч болзошгүй нөхцөл байдал үүсээд байна. Тиймээс Ерөнхий сайдын зүгээс бүхий л боломжоо ашиглан, төсөвт хэмнэлт гаргах шаардлагатайг Сангийн сайдад даалгасан. Үүнд:

Ерөнхийлөгч, Ерөнхий сайд, УИХ-ын даргаас гадна гишүүд, нийслэлийн болон аймгийн Засаг дарга нар, орлогч нарын хамт, ИТХ-ын дарга зэрэг багтах юм. Товчоор хэлбэл улс төрийн томилгоогоор төрийн өндөр албан тушаалд очсон бүх хүн цалингийнхаа 30 хувийг төсөвт нэмэрлэхэ гэсэн үг. Энд нэг зүйлийг тодотгоход төрийн албан тушаалтан гэхээр төрийн албан хаагчид тэр дундаа, сургуулийн захирал багтана гэж ойлгоод байгаа нь буруу бөгөөд төрийн үйлчилгээний албан тушаалтнууд цалингаа хасуулахгүй. Харин одоо цалингаа хасуулах хүмүүстэй танилцъя. Төрийн албаны хуульд зааснаар төрийн өндөр албан тушаалтан 224 хүн байна. Үүнд

ТӨ- I Ерөнхийлөгч

ТӨ- II УИХ-ын дарга, Ерөнхий сайд,

ТӨ- III УИХ-ын дэд дарга, Үндсэн хуулийн Цэцийн дарга, Улсын дээд шүүхийн Ерөнхий шүүгч

ТӨ- IV /99/

УИХ-ын гишүүд, Засгийн газ-рын сайд нар, Улсын Ерөнхий прокурор, нийслэлийн ИТХ-ын Тэргүүлэгчдийн дарга, нийс-лэлийн Засаг дарга бөгөөд Улаан-баатар хотын захирагч, Шүүхийн ерөнхий зөвлөлийн дарга, Монгол Улсын Ерөнхий аудитор, АТГ-ын дарга,

ТӨ- V /68/

Ерөнхийлөгчийн Тамгын газрын дарга, Засгийн газрын Хэрэг эрхлэх газрын дарга, УИХ-ын Тамгын газрын Ерөнхий нарийн бичгийн дарга, Үндсэн хуулийн цэцийн гишүүн /ес/, Улсын дээд шүүхийн шүүгч, аймгийн ИТХ-ын Тэргүүлэгчдийн дарга /21/, аймгийн Засаг дарга /21/, Төрийн албаны зөвлөлийн дарга, Шүүхийн ерөнхий зөвлөлийн гишүүн /дөрөв/, Үндэсний аюулгүй байдлын зөвлөлийн нарийн бичгийн дарга, Монголбанкны Ерөнхийлөгч, Санхүүгийн зохицуулах хорооны дарга, Үндэсний статистикийн газрын дарга, Монгол Улсын Ерөнхий прокурорын орлогч, ХЭҮК-ын дарга, СЕХ-ны дарга, АТГ-ын дэд дарга

ТӨ-VI /50/

Дэд сайд /17/, Ерөнхийлөгчийн зөвлөх /найм/, УИХ-ын даргын зөвлөх /дөрөв/, Ерөнхий сайдын зөвлөх /долоо/, Шүүхийн ерөнхий зөвлөлийн гүйцэтгэх нарийн бичгийн дарга, Төрийн албаны зөвлөлийн орон тооны гишүүн /хоёр/, Монголбанкны дэд ерөнхийлөгч, Монгол Улсын Ерөнхий аудиторын орлогч, Үндэсний статистикийн газрын дэд дарга, ХЭҮК-ын гишүүн /гурав/, Санхүүгийн зохицуулах хорооны орон тооны гишүүн /дөрөв/,

Сонгуулийн ерөнхий хорооны нарийн бичгийн дарга зэрэг багтаж байна. ТӨ-I-VI-д заасан төрийн өндөр албан тушаалтны цалинг ТЗ-14 /төрийн захиргаа/ буюу Төрийн нарийн бичгийн даргын цалинд суурилан, тооцож боддог юм байна. Харин албан тушаалын сарын цалинг итгэлцүүрийн дагуу тооцож үзвэл:

ТӨ-I цалин 2 319 274 төгрөг.

ТӨ-II цалин 1748110 төгрөг,

ТӨ-III цалин 1341371 төгрөг, нийт дөрвөн албан тушаалтан 5 365 484 төгрөг

ТӨ-IV цалин 1289447 төгрөг, нийт 99 албан тушаалтан 127 655 253 төгрөг

ТӨ- V цалин 1194253 төгрөг, нийт 68 албан тушаалтан 81 209 204 төгрөг

ТӨ-VI цалин 1142329 төгрөг, нийт 50 албан тушаалтан 57 116 450 төгрөг

Эндээс үзвэл төрийн өндөр албан тушаалтнуудын сарын цалин нийт 277 161 885 төгрөг болдог байна. Энэхүү мөнгийг гурван сараар үржүүлбэл 831 485 655 төгрөг байх бөгөөд Ерөнхий сайдын санал гаргасан төрийн өндөр албан тушаалтны цалинг гурван сар 30 хувиар хасахад 249 сая 445 мянган төгрөг хэмнэх тооцоо харагдаж байгаа юм. Хуульд төрийн өндөр албан тушаалтан гэж хэнийг хэлснээс харж, тооцоолбол ийм тоо гарч байгаа юм. Гэхдээ ажлын хэсэг дээр ТӨ I-IV хүртэлх албан тушаалтныг оролцуулах эсэхээс хамаарч дээрх тоонд өөрчлөлт гарах магадлалтай. Ямартай ч дээрх тооцоллоос харвал 300-гаад сая төгрөгийг хэмнэх боломжтой байна. Дээрх мөнгөн дүнг ажлын хэсэг бага байна гэж үзвэл төрийн өндөр албан тушаалтнуудыг нэмж тооцсоноор төсөвт орж ирэх мөнгөн дүнгийн тоог нэмэгдүүлэх боломжтой юм.

SHA256 00ddae5bbc2ddf29954749519ecfb3978a68db6237ebea8e646a898c353053ce

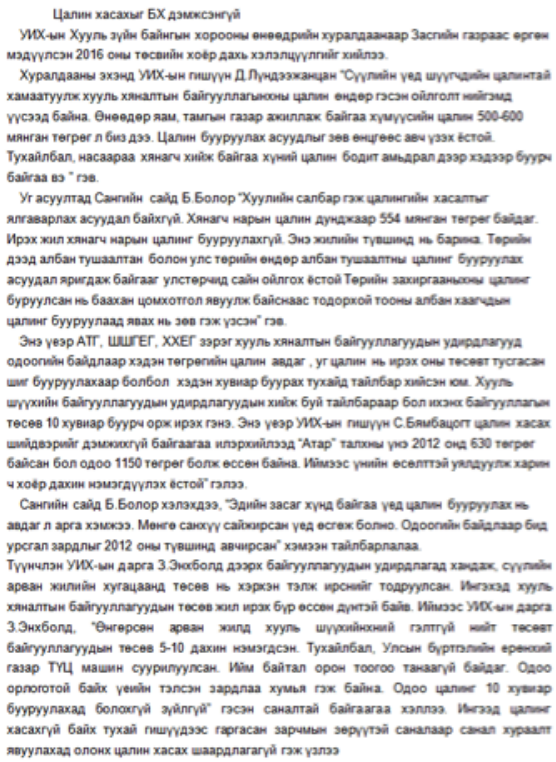
Date	10/22/2015
Filename	Улс төрийн www.politik.mn сайт нээгдлээ.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Weaponized Microsoft Word document found titled 'Улс төрийн www.politik.mn сайт нээгдлээ.doc' (States opens state www.politik.mn site.doc). Likely delivered via spear-phishing. CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy document dropped by the malicious file discusses a new website being launched by the Mongolian government.

Улс төрийн www.politik.mn сайт нээгдлээ

УИХ-аар 2015 оны төсвийн тодотгол, 2016 оны төсвийн төслийг хэлэлцэж, Г.Уянга гишүүн Ерөнхий сайдыг оцруулахаар гарын үсэг цуглуулж, улстөр донсолж буй энэ халуун өдрүүдэд Монголын хамгийн отгон www.politik.mn мэдээллийн сайт уншигдад мэдээллээ түгээж эхэллээ. Монголын улс төрийн амьдралын бүхий л үйл явцыгтэрэл, сүүдэртэй нь олон нийтэд илчлэн дэлгэх, өөр өөр байр суурийг эсрэцүүлэн харуулах зорилготой шинэ сайт улс төрийн анхны төрөлжсөнмэдээллийн хэрэгсэл гэдгээрээ өрсөлдөгчдөөсөө ялгарахыг зорьж буй юм байна.

Тус сайтыг Монголын хамгийн олон уншигчтай www.news.mn сайтын тойм, нийтлэлчээр ажиллаж байсан З.Боргилмаа нарын сэтгүүлчдийн баг санаачлан байгуулжээ. Шинэ сайтын мэдээлэлтэй танилцах бол www.politik.mnхаягаар хандах боломжтой. Тухайлбал, өнөөдрийн онцлох сэдэвтээ Засгийн газрын бүтцийн өөрчлөлтийн талаар хэнден бичсэнийг ЭНЭХҮҮ холбоосоор дэлгэрүүлэн уншина уу.

SHA256	c2ebaf4366835e16f34cc7f0b56f8eaf80a9818375c98672bc678bb4107b4d8c
Date	10/28/2015
Filename	Unknown
Vulnerability Targeted	CVE-2012-0158
Tools Used	Cmstar
Description	Weaponized Microsoft Word document with unknown title found. Likely delivered via spear-phishing. CVE-2012-0158 exploit used, dropping new variant of Cmstar. The decoy document talks about a 2016 budget discussion in the Mongolian Parliament.



Цалин хасахыг БХ дэмжсэнгүй

УИХ-ын Хууль зүйн байнгын хорооны өнөөдрийн хуралдаанаар Засгийн газраас өргөн мэдүүлсэн 2016 оны төсвийн хоёр дахь хэлэлцүүлгийг хийлээ.

Хуралдааны эхэнд УИХ-ын гишүүн Д.Лүндээжанцан "Сүүлийн үед шүүгчдийн цалинтай хамаатуулж хууль хяналтын байгууллагынхны цалин өндөр гэсэн ойлголт нийгэмд үүсээд байна. Өнөөдөр яам, тамгын газар ажиллаж байгаа хүмүүсийн цалин 500-600 мянган төгрөг л биз дээ. Цалин бууруулах асуудлыг зөв өнцгөөс авч үзэх ёстой. Тухайлбал, насаараа хянагч хийж байгаа хүний цалин бодит амьдрал дээр хэдээр буурч байгаа вэ " гэв.

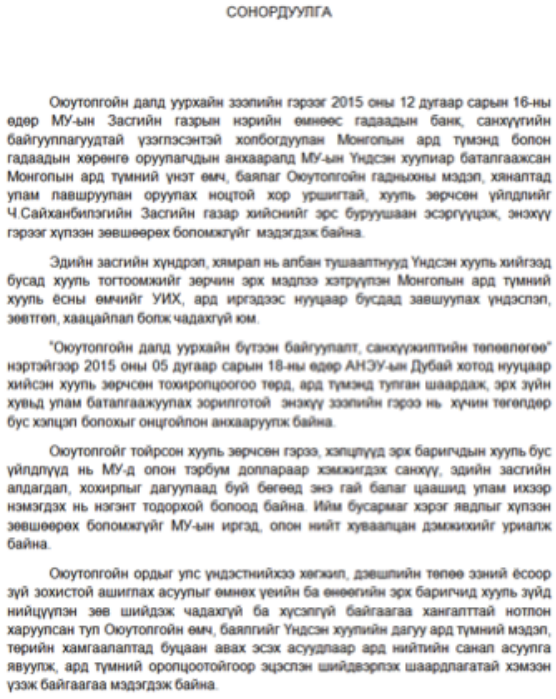
Уг асуултад Сангийн сайд Б.Болор "Хуулийн салбар гэж цалингийн хасалтыг ялгаварлах асуудал байхгүй. Хянагч нарын цалин дунджаар 554 мянган төгрөг байдаг. Ирэх жил хянагч нарын цалинг бууруулахгүй. Энэ жилийн түвшинд нь барина. Төрийн дээд албан тушаалтан болон улс төрийн өндөр албан тушаалтны цалинг бууруулах асуудал яригдаж байгаа улстөрчид сайн ойлгох ёстой Төрийн захиргааныхны цалинг бууруулсан нь баахан цомхотгол явуулж байснаас тодорхой тооны албан хаагчдын цалинг бууруулаад явах нь зөв гэж үзсэн" гэв.

Энэ үеэр АТГ, ШШГЕГ, ХХЕГ зэрэг хууль хяналтын байгууллагуудын удирдлагууд одоогийн байдлаар хэдэн төгрөгийн цалин авдаг , уг цалин нь ирэх оны төсөвт тусгасан шиг бууруулахаар болбол хэдэн хувиар буурах тухайд тайлбар хийсэн юм. Хууль шүүхийн байгууллагуудын удирдлагуудын хийж буй тайлбараар бол ихэнх байгууллагын төсөв 10 хувиар буурч орж ирэх гэнэ. Энэ үеэр УИХ-ын гишүүн С.Бямбацогт цалин хасах шийдвэрийг дэмжихгүй байгаагаа илэрхийлээд "Атар" талхны үнэ 2012 онд 630 төгрөг байсан бол одоо 1150 төгрөг болж өссөн байна. Иймээс үнийн өсөлттэй уялдуулж харин ч хоёр дахин нэмэгдүүлэх ёстой" гэлээ.

Сангийн сайд Б.Болор хэлэхдээ, "Эдийн засаг хүнд байгаа үед цалин бууруулах нь авдаг л арга хэмжээ. Мөнгө санхүү сайжирсан үед өсгөж болно. Одоогийн байдлаар бид урсгал зардлыг 2012 оны түвшинд авчирсан" хэмээн тайлбарлалаа.

Түүнчлэн УИХ-ын дарга З.Энхболд дээрх байгууллагуудын удирдлагад хандаж, сүүлийн арван жилийн хугацаанд төсөв нь хэрхэн тэлж ирснийг тодруулсан. Ингэхэд хууль хяналтын байгууллагуудын төсөв жил ирэх бүр өссөн дүнтэй байв. Иймээс УИХ-ын дарга З.Энхболд, "Өнгөрсөн арван жилд хууль шүүхийнхний гэлтгүй нийт төсөвт байгууллагуудын төсөв 5-10 дахин нэмэгдсэн. Тухайлбал, Улсын бүртгэлийн ерөнхий газар ТҮЦ машин суурилуулсан. Иймэрхүү байтал орон тоогоо танаагүй байдаг. Одоо орлоготой байх үеийн тэлсэн зардлаа хумья гэж байна. Одоо цалинг 10 хувиар бууруулахад болохгүй зүйлгүй" гэсэн саналтай байгаагаа хэллээ. Ингэхэд цалинг хасахгүй байх тухай гишүүдээс гаргасан зарчмын зөрүүтэй саналаар санал хураалт явуулахад олонх цалин хасах шаардлагагүй гэж үзлээ

SHA256	aa86f4587423c2ff677aebae604614030f9f4d38280409501662ab4e4fe20c2a
Date	12/23/2015
Filename	СОНОРДУУЛГА.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	BBSRAT
Description	Weaponized Microsoft Word document found titled 'СОНОРДУУЛГА.doc' (Announcement). Likely delivered via spear-phishing. CVE-2012-0158 exploit used, with BBSRAT embedded. The document translates to an announcement of a loan agreement signed with foreign banks and financial institutions on October 16th, 2015.



СОНОРДУУЛГА

Оюутолгойн далд уурхайн зэвлийн гэрээг 2015 оны 12 дугаар сарын 16-ны өдөр МУ-ын Засгийн газрын нэрийн өмнөөс гадаадын банк, санхүүгийн байгууллагуудтай үзэглэсэнтэй холбогдуулан Монголын ард түмэнд болон гадаадын хөрөнгө оруулагчдын анхаарлад МУ-ын Үндсэн хуулиар батлагаажсан Монголын ард түмний үнэт өмч, баялаг Оюутолгойн гадныхны мэдэл, хяналтад улам лавшруулан оруулах ноцтой хор уршигтай, хууль зөрчсөн үйлдлийг Ч.Сайханбилэгийн Засгийн газар хийснийг эрс буруушаан эсэргүүцэж, энэхүү гэрээг хүлээн зөвшөөрөх боломжгүйг мэдэгдэж байна.

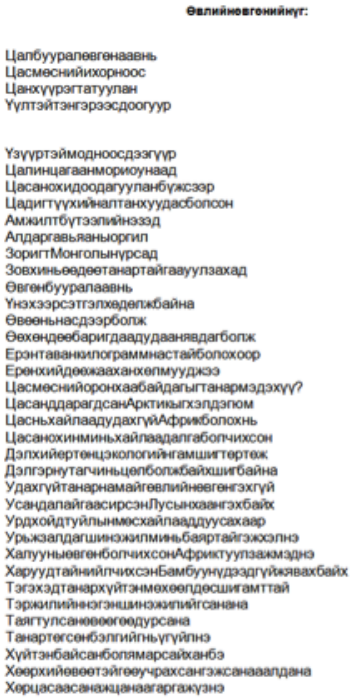
Эдийн засгийн хүндрэл, хямрал нь албан тушаалтнууд Үндсэн хууль хийгээд бусад хууль тогтоомжийг зөрчин эрх мэдлээ хэтрүүлэн Монголын ард түмний хууль ёсны өмчийг УИХ, ард иргэдээс нууцаар бусдад завшуулах үндэслэл, зөвтгөл, хаацайлал болж чадахгүй юм.

"Оюутолгойн далд уурхайн бүтээн байгуулалт, санхүүжилтийн төлөвлөгөө" нэртэйгээр 2015 оны 05 дугаар сарын 18-ны өдөр АНЭУ-ын Дубай хотод нууцаар хийсэн хууль зөрчсөн тохиролцоогоо төрд, ард түмэнд тулган шаардаж, эрх зүйн хүчээд улам баталгаажуулах зорилготой энэхүү зэвлийн гэрээ нь хүчин төгөлдөр бус хэлцэл болохыг онцгойлон анхаарууллж байна.

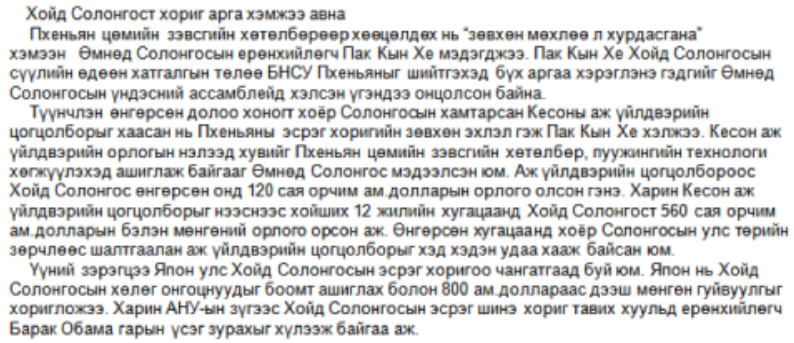
Оюутолгойг тойрсон хууль зөрчсөн гэрээ, хэлцлүүд эрх баригчдын хууль бус үйлдлүүд нь МУ-д олон тэрбум долларааар хэмжигдэх санхүү, эдийн засгийн алдагдал, хохирлыг дагуулаад буй бөгөөд энэ гай балаг цаашид улам ихээр нэмэгдэх нь нэгэнт тодорхой болоод байна. Иймээс бусармаг хэрэг явдлыг хүлээн зөвшөөрөх боломжгүйг МУ-ын иргэд, олон нийт хуваалцан дэмжихийг уриалж байна.

Оюутолгойн ордыг улс үндэстнийхээ хөгжил, дэвшлийн төлөө эзний ёсоор зүй зохистой ашиглах асуулыг өмнөх үеийн ба өнөөгийн эрх баригчид хууль зүйд нийцүүлэн зөв шийдэж чадахгүй ба хүсэлгүй байгаагаа хангалттай нотлон харуулсан тул Оюутолгойн өмч, баялгийг Үндсэн хуулийн дагуу ард түмний мэдэл, төрийн хамгаалалтад буцаан авах эсэх асуудлаар ард нийтийн санал асуулга явуулж, ард түмний оролцоотойгоор эцэслэн шийдвэрлэх шаардлагатай хэмээн үзэж байгаагаа мэдэгдэж байна.

SHA256	fc21814a5f9ed2f6bef9e15b113d00f9291a6553c1e02cc0b4c185c6030eca45
Date	1/4/2016
Filename	Өвлийн өвгөнийн үг.doc
Vulnerability Targeted	CVE-2012-0158
Tools Used	BBSRAT
Description	Weaponized Microsoft Word document found titled 'Өвлийн өвгөнийн үг.doc' (Santa's word). Likely delivered via spear-phishing. CVE-2012-0158 exploit used, with BBSRAT embedded. The decoy document, which had spacing removed for an unknown reason, provides a series of children holiday season songs and poems.



SHA256	7e031a04e570cddda907d0b4b7af19ce60dc481394dfb3813796ce0e6d079305	**Date**	2/17/2016
Filename	Хойд Солонгост хориг арга хэмжээ авна.doc		
Vulnerability Targeted	CVE-2012-0158 and CVE-2014-1761		
Tools Used	Cmstar and BBSRAT		
Description	Weaponized Microsoft Word document found titled 'Хойд Солонгост хориг арга хэмжээ авна.doc' (North Korea sanctions). Exploits for both CVE-2012-0158 and CVE-2014-1761 used, dropping a separate, newer variant of Cmstar which downloaded BBSRAT as its final payload. The decoy document talks about a recent speech made by the South Korean President regarding sanctions made against North Korea.		



Хойд Солонгост хориг арга хэмжээ авна

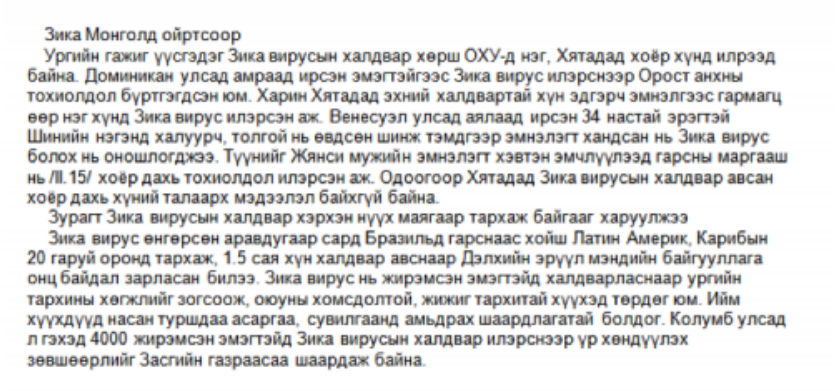
Пхеньян цөмийн зэвсгийн хөтөлбөрөөр хөөцөлдөх нь "зөвхөн мөхлөө л хурдасгана" хэмээн Өмнөд Солонгосын ерөнхийлөгч Пак Кын Хе мэдэгджээ. Пак Кын Хе Хойд Солонгосын сүүлийн едөөн хатгалгын төлөө БНСУ Пхеньяныг шийтгэхэд бүх аргаа хэрэглэнэ гэдгийг Өмнөд Солонгосын үндэсний ассамблейд хэлсэн үгэндээ онцолсон байна.

Түүнчлэн өнгөрсөн долоо хоногт хоёр Солонгосын хамтарсан Кесоны аж үйлдвэрийн цогцолборыг хаасан нь Пхеньяны эсрэг хоригийн зөвхөн эхлэл гэж Пак Кын Хе хэлжээ. Кесон аж үйлдвэрийн орлогын нэлээд хувийг Пхеньян цөмийн зэвсгийн хөтөлбөр, пуужингийн технологи хөгжүүлэхэд ашиглаж байгааг Өмнөд Солонгос мэдээлсэн юм. Аж үйлдвэрийн цогцолбороос Хойд Солонгос өнгөрсөн онд 120 сая орчим ам.долларын орлого олсон гэнэ. Харин Кесон аж үйлдвэрийн цогцолборыг нээснээс хойших 12 жилийн хугацаанд Хойд Солонгост 560 сая орчим ам.долларын бэлэн мөнгөний орлого орсон аж. Өнгөрсөн хугацаанд хоёр Солонгосын улс төрийн зөрчлөөс шалтгаалан аж үйлдвэрийн цогцолборыг хэд хэдэн удаа хаажж байсан юм.

Үүний зэрэгцээ Япон улс Хойд Солонгосын эсрэг хоригоо чангатгаад буй юм. Япон нь Хойд Солонгосын хөлөг онгоцнуудыг боомт ашиглах болон 800 ам.долларааc дээш мөнгөн гуйвуулгыг хоригложээ. Харин АНУ-ын зүгээс Хойд Солонгосын эсрэг шинэ хориг тавих хуульд ерөнхийлөгч Барак Обама гарын үсэг зурахыг хүлээж байгаа аж.

SHA256	5c7e3cde4d286909154e9a5ee5a5d061a1f0efaa9875fb50c9073e1e8b6cfaef
Date	2/19/2016
Filename	Зика Монголд ойртсоор.doc

Vulnerability Targeted	CVE-2012-0158 and CVE-2014-1761
Tools Used	Cmstar and BBSRAT
Description	Weaponized Microsoft Word document found titled 'Зика Монголд ойртсоор' (Zika closer to Mongolia). Exploits for both CVE-2012-0158 and CVE-2014-1761 used, dropping a separate, newer variant of Cmstar which downloaded BBSRAT as its final payload. The translated Mongolian text found within the decoy document discusses how the Zika virus has been witnessed in both China and Russia, as well as other countries across the globe.



Зика Монголд ойртсоор

Ургийн гажиг үүсгэдэг Зика вирусын халдвар хөрш ОХУ-д нэг, Хятадад хоёр хүнд илрээд байна. Доминикан улсад амраад ирсэн эмэгтэйгээс Зика вирус илэрснээр Орост анхны тохиолдол бүртгэгдсэн юм. Харин Хятадад эхний халдвартай хүн эдгэрч эмнэлгээс гармагц өөр нэг хүнд Зика вирус илэрсэн аж. Венесуэл улсад аялаад ирсэн 34 настай эрэгтэй Шинийн нэгэнд халуурч, толгой нь өвдсөн шинж тэмдгээр эмнэлэгт хандсан нь Зика вирус болох нь оношлогджээ. Түүнийг Жянси мужийн эмнэлэгт хэвтэн эмчлүүлээд гарсны маргааш нь /II.15/ хоёр дахь тохиолдол илэрсэн аж. Одоогоор Хятадад Зика вирусын халдвар авсан хоёр дахь хүний талаарх мэдээлэл байхгүй байна.

Зураг Зика вирусын халдвар хэрхэн нүүх маягаар тархаж байгааг харуулжээ

Зика вирус өнгөрсөн аравдугаар сард Бразильд гарснаас хойш Латин Америк, Карибын 20 гаруй оронд тархаж, 1.5 сая хүн халдвар авснаар Дэлхийн эрүүл мэндийн байгууллага онц байдал зарласан билээ. Зика вирус нь жирэмсэн эмэгтэйд халдварласнаар ургийн тархины хөгжлийг зогсоож, оюуны хомсдолтой, жижиг тархитай хүүхэд төрдөг юм. Ийм хүүхдүүд насан туршдаа асаргаа, сувилгаанд амьдрах шаардлагатай болдог. Колумб улсад л гэхэд 4000 жирэмсэн эмэгтэйд Зика вирусын халдвар илэрснээр үр хөндүүлэх зөвшөөрлийг Засгийн газраасаа шаардаж байна.

SHA256	0b0e6b40a63710b4f7e6d00d7a4a86e6db2df720fef48640ab6d9d88352a4890
Date	2/19/2016
Filename	Хятадад “Зика” вирусын хоёр дахь тохиолдол илэрчээ.doc
Vulnerability Targeted	CVE-2012-0158 and CVE-2014-1761
Tools Used	Cmstar and BBSRAT
Description	Weaponized Microsoft Word document found titled 'Хятадад “Зика” вирусын хоёр дахь тохиолдол илэрчээ' (China "Zika" viruses in two cases). Exploits for both CVE-2012-0158 and CVE-2014-1761 used, dropping a separate, newer variant of Cmstar which downloaded BBSRAT as its final payload. The dropped decoy document contains a press release dated on February 16th, 2016. The press release discusses changes made to the coal industry in inner Mongolia, The G-20 meeting in China, a five year plan for economic and social development, and two cases of the Zika virus.

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ХЭВЛЭЛИЙН ТОЙМ

2016 оны 2 дугаар сарын 16-ны өдөр

Бээжин хот

ӨМӨЗО нүүрсний салбарын өөрчлөлтийг хийж байна

Сүүлийн жилүүдэд Хятадын эдийн засгийн өсөлт буурч, нүүрсний салбарт "хахир өвөл" ирсэнтэй холбогдуулан ӨМӨЗО "нүүрсээ ухаж нүүрс зардаг" байдлыг өөрчилж, нэмүү өртөг шингэсэн эргэлтэд оруулах замд ороод байна. "Нүүрсний хар нунтгийг цэвэр ус шиг өнгөтэй түлш болгон үйлдвэрлэж байна" хэмээн "Шэньхуа" корпорацийн дэд ерөнхий захирал Шу Гөпинь хэлсэн байна. Энэ нь дэлхийд хамгийн анхны сая тоннын хүчин чадалтай нүүрс шингэрүүлэх төхөөрөмж аж. 2015 онд 700 мянган тн түлш боловсруулсан байна. Нүүрснээс шингэрүүлсэн түлш гаргах, байгалийн хий гаргах, нүүрсийг гүн боловсруулах төслүүд Өвөр Монголд ажил хэрэг болж, 13-р таван жилийн төлөвлөгөөний төгсгөлд нүүрс боловсруулах үйлдвэрлэл одоогийн 30 хувиас 50 хувьд хүрэх юм байна. Гар утасны сэлбэг, цемийн зөчим хүчний түлш, биополийн эмийн бэлдмэл, тоног төхөөрөмжийн үйлдвэрлэл нь Өвөр Монголын эдийн засгийн өсөлтийн шинэ үзүүлэлтүүд болоод байна. 2015 онд ӨМӨЗО-ны өндөр технологийн аж үйлдвэрийн өсөлт өнгөрсөн оны мөн үеэс 23,5 хувиар өссөн байна. Нүүрсний үйлдвэрлэл нь Өвөр Монголын аж үйлдвэрлэлийн 50 хувийг өмнө нь эзлэж байсан бол одоо 23 хувийг эзлэж байна. 13-р таван жилийн явцад нүүрсний үйлдвэрлэлийн эзлэх хувийг бууруулж 15 хувьд хүргэх зорилт тавьсан байна. Бүхэл бүтэн системийн өөрчлөлт хийснээр "нүүрснээс харааг" аж үйлдвэрийн салбарыг хямралаас гаргахаар ажиллах юм байна.

Рэньминь рибао 2016.2.16

G20-ийн уулзалт Хятадад болно

G20-ийн орнуудын 11 дэх удаагийн дээд түвшний уулзалт энэ оны 9 дүгээр сарын 4-5-ны өдрүүдэд БНХАУ-ын Жөзян мужийн Ханжоу хотноо зохион байгуулагдана. Уулзалтын бэлтгэл ажлыг хариуцсан Төрийн Зөвлөлийн пишүүн Ян Зечы уулзалтын бэлтгэлийн талаар сэтгүүлчдийн асуултад хариулт өгсөн байна. Тэрээр "Энэ удаагийн уулзалтын гол сэдэв нь "Шинийг санаачлах, идэвхтэй, хамтдаа урагшлах, хүртээмжтэй дэлхийн эдийн засаг". Гол зорилго нь дэлхийн эдийн засаг, улс орнуудын хөгжлийн шаардлага, тогтвортой хөгжлийг хангах гэж Си Зиньлин дарга хэлсэн" гэсэн байна. G20-ийн уулзалт дэлхийн эдийн засаг, олон улсын эдийн засгийн хамтын ажиллагаанд чухал үүрэг гүйцэтгэдэг. 2008 оны 11 дүгээр сард анх

The Digital Quartermaster: Tool Overlap

The tools we observed being used in this attack campaign remained consistent throughout the six months of data we were able to collect and analyze. Yet, prior to the findings in this report, none of the tools used in this campaign had been observed being used in conjunction with each other. In their 2013 report, Kaspersky theorized that NetTraveler may have had connections to the Lurid/Enfal adversaries due to some similarities in command and control infrastructure and targeting of minority groups in China, but no strong evidence was discovered since then. CMStar is a variant of Lurid discovered by us in May 2015, with similar targeting as previously observed as NetTraveler, but again, with no strong connections. BBSRAT is a relatively new Trojan we had discovered and publicized in December 2015 and had attributed it to a campaign dubbed ‘Roaming Tiger’ by ESET in 2014, which specifically appeared to target Russia and Russian speaking nation state. None of these tools have been publicly observed in use together, in a singular campaign, until now:

- The initial dropper embedded in the weaponized document files were obfuscated using a subtraction cipher previously used to obfuscate strings in the NetTraveler malware family.
- A BinDiff comparison of the newer Cmstar variant with a previously reported on NetTraveler sample shows an 80% code similarity
- The first stage loader used in the attacks was Cmstar, or lightly modified variants. Cmstar is closely related to Lurid which is associated with the Enfal trojan
- The final payload for the newest weaponized documents retrieved was BBSRAT, which was previously associated with an attack campaign called "Roaming Tiger", targeting Russia and other Russian speaking nations speaking

The one commonality that does appear amongst these seemingly different tools used by different operators is their geolocational nexus: China. In 2011, TrendMicro strongly attributed Lurid/Enfal to operators based out of China, although they stopped just short of claiming it. In Kaspersky’s 2013 report on NetTraveler, another strong

attribution was made to a China-based operator. ESET's "Roaming Tiger" reporting did not attribute the attack to any specific nation-state, but examining the command and control infrastructure and WHOIS data again suggested a China-based operator.

These facts begin to lead us to the following possible conclusions: the previous attack campaigns associated with their specific tool were all actually conducted by one, large, all encompassing operations unit. The previous attack campaigns were conducted by separate, but related operations unit with access to a common Digital Quartermaster for tools, or some combination of either scenario.

Technical Analysis of Tools Used

All of the Microsoft Word documents leveraged in these attacks used the CVE-2012-0158 and CVE-2014-1761 exploits. All of the exploit documents, in addition to targeting the same organizations and relying upon the same exploit techniques, ultimately dropped a version of the BBSRAT. A large number of the encountered samples used a new version of the Cmstar downloader to accomplish this, while some documents dropped and executed BBSRAT directly. Upon successful exploitation, the exploit documents would drop and execute a payload using one of the following techniques:

1. The exploit document drops and executes a file with a path of %TEMP%\xpsfiltsvcs.tmp. This file contains an original Cmstar downloader that was discussed in a previous blog post.
2. The 'MSOProtect.acl', 'offcln.log', and 'offcln.pip' files are dropped in the %APPDATA%\Microsoft\Office\ directory. The MSOProtect.acl file contains a new variant of the Cmstar malware family. The offcln.pip is a DLL that is responsible for opening a legitimate Microsoft Word decoy document. The offcln.log file contains a command that will open this decoy document. The offcln.log file is used by offcln.pip in order to accomplish this.
3. The %APPDATA%\comctl32.dll file is dropped and subsequently loaded. This file contains either a new instance of the Cmstar downloader, or a copy of the BBSRAT malware family, which was discussed by Palo Alto Networks in December 2015.

New Cmstar Downloader

The majority of the spear-phishing attachments leveraged variants of the previously discussed downloader named 'Cmstar'. Much of the functionality remained consistent in the newest variants, which were compiled in July and August of 2015. For reference, the original Cmstar downloader malware samples were compiled in February 2015.

The new samples appear to have minimal changes made, and in fact a number of the debugging statements mentioned in the original samples are seen in a number of the newest variants. The obfuscated routine that is responsible for downloading the payload has increased in size from 779 bytes to 943 bytes. This increase in size is due to additional error controls put into place. This routine is still encrypted using a single-byte XOR operation.

However, the newest Cmstar variants use a different routine to obfuscate important strings within the binary. The following code, represented in Python, accomplishes this:

```
1  def decode(data):
2    out = ""
3    c = 0
4    for d in data:
5      out += chr(ord(d) - c - 10)
6      c += 1
7    return out
```

Malware analysts may recognize this routine, as it's identical to the one witnessed in previously discussed NetTraveler samples that were found to be targeting an individual working for the Foreign Ministry of Uzbekistan in China. As witnessed in the following diagram, the new Cmstar downloader's obfuscation routine has a 100% code match to the NetTraveler downloader previously encountered:

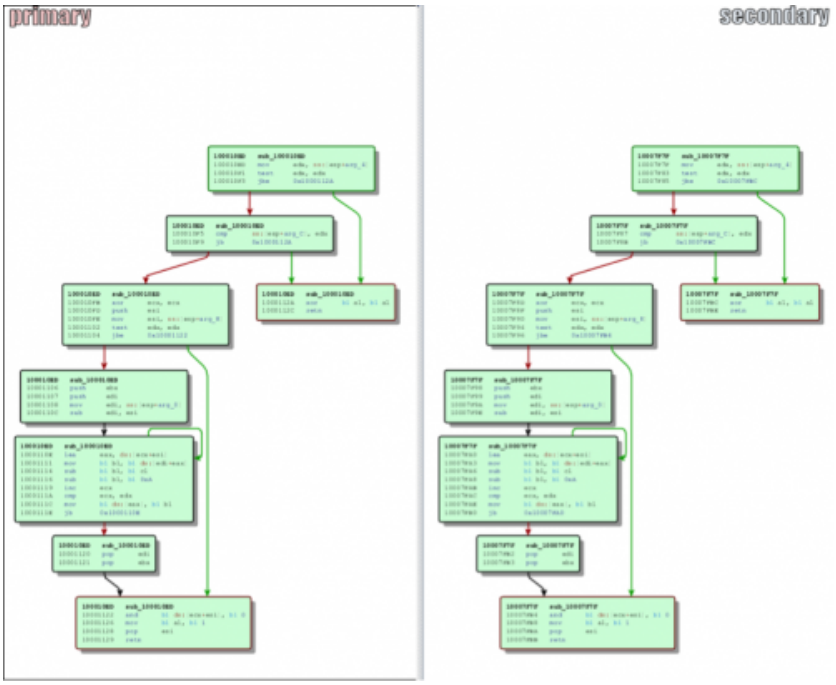


Figure 1 Code Overlap Between Cmstar and NetTraveler Downloaders

The following URLs were identified to be used by these Cmstar samples:

- http://thbaw.ofhloe[.]com/cgl-bin/conime.cgi
- http://dolimy.celeinkec[.]com/cgl-bin/upl.cgi
- http://question.eboregi[.]com
- http://pplime.savecarrots[.]com/cgl-bin/upsd.cgi
- http://dolimy.celeinkec[.]com/bin/r0206/update.tmp

The majority of these URLs were not responsive at the time of analysis, with the exception of the last one. This returned file is an encoded executable that contains a dropper, which in turn loads BBSRAT.

BBSRAT

Much of BBSRAT's functionality has remained consistent in the newest variants. Like previous versions, the malware will build an Import Address Table at runtime and uses the following mutex to ensure a single copy of BBSRAT is running at a given time:

Global\\GlobalAcProtectMutex

Additionally, the network structure, URL pattern, and other characteristics of the malware remain consistent. BBSRAT will ensure persistence by setting the following registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\comctl32 - rundll32.exe %APPDATA%\comctl32.dll, Enter

The largest modification has been the addition of four commands to the command and control handler. These commands are still being researched and full functionality of them has yet to be determined. We have identified the following BBSRAT command and control servers:

- cocolco[.]com
- ofhloe[.]com
- housejjk[.]com

Infrastructure Analysis

Mapping out the first stage command and control infrastructure for the analyzed Cmstar samples revealed an infrastructure that was most likely deployed specifically for this attack campaign:

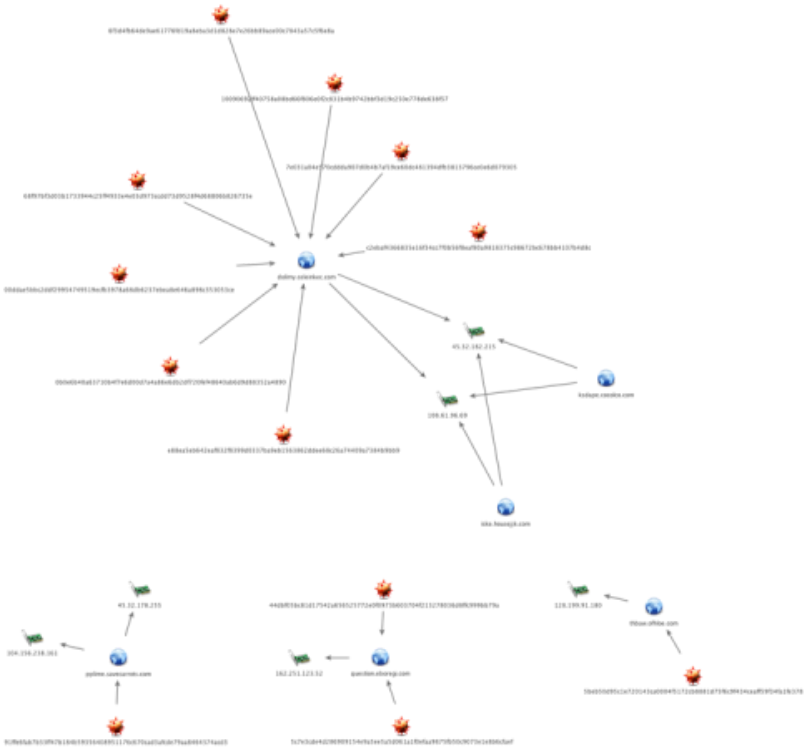


Figure 2 Cmstar Command and Control Infrastructure

A single domain, question.erobegi[.]com, was found to be reused. This domain had previous been identified as a first stage command and control in May 2015 when we initially discovered CMStar. However, the payload was not identified at the time. The WHOIS data revealed heavy usage of resellers by the adversary, likely as an evasion technique. Analyzing the historical WHOIS data however, revealed one of the 'clean' personas used by the adversary as a registrant 'HELENEHELEN@EXCITE.CO.JP', was used to register one of the command and control domains for CMStar, celeinkec[.]com as well as one of the primary command and control domains for BBSRAT, housejjk[.]com, further supporting the links between CMStar, and BBSRAT.

The BBSRAT command and control infrastructure remained exactly the same as previously reported in December 2015:

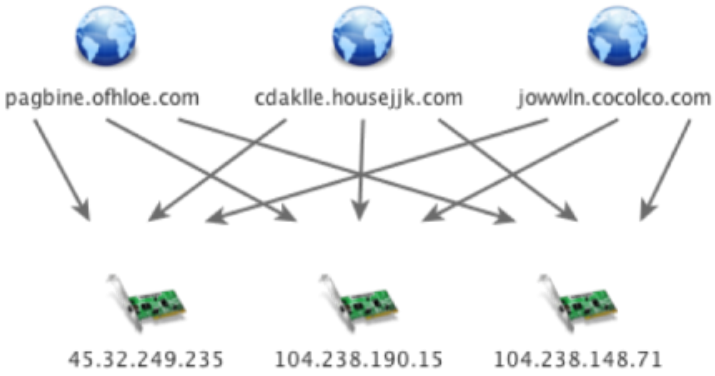


Figure 3 BBSRAT Command and Control Infrastructure

Unfortunately, we were unable to retrieve all of the final payloads from every sample at the time of analysis. One interesting fact to note is the use of the primary domain ofhloe[.]com; BBSRAT uses pagbine.ofhloe[.]com as a primary command and control, while we also observed Cmstar thbaw.ofhloe[.]com as a first stage command and control to likely retrieve BBSRAT.

Conclusion

Unit 42 often speaks of sharing threat intelligence, tools, and procedures amongst the security industry, often times pointing to the fact that the adversaries we are up against on an everyday basis are doing the exact same. Still, as a community, when we do publicize adversary groups or campaigns, there is a tendency to encapsulate each and place them in their own isolated bubbles, directly contradicting the message of sharing amongst the adversary. The reasoning behind this is not meant to be hypocritical – it is simply more straightforward for identification and ingestion purposes to be able to silo each group or campaign rather than come to the conclusion that *every* group or campaign is somehow related due to the sharing nature of the adversaries. We must acknowledge the fact however, that in general many attacks *are* related, even if they do appear significantly different or do not share the same TTPs as observed previously

The collection of data we have analyzed strongly points to the fact that a Digital Quartermaster may exist amongst the adversary. The strong overlaps within the tactics used in the toolsets as well as links in infrastructure indicate it is likely that a singular entity is responsible for deployment and maintenance of the tools used, in conjunction with a separate operator group responsible for the actual execution of the cyber espionage operations.

Palo Alto Networks customers are protected through our next-generation security platform:

- WildFire successfully detects BBSRAT, Cmstar, and the weaponized documents as malicious
- AutoFocus identifies the tools used under the Cmstar and BBSRAT tags
- Traps actively detects and prevents exploitation of both CVE-2012-0158 and CVE-2014-1761
- The C2 domains and files mentioned in this report are blocked through Threat Prevention

Indicators of Compromise

Exploit Document SHA256 Hashes

5beb50d95c1e720143ca0004f5172cb8881d75f6c9f434ceaff59f34fa1fe378
10090692ff40758a08bd66f806e0f2c831b4b9742bbf3d19c250e778de638f57
44dbf05bc81d17542a656525772e0f0973b603704f213278036d8ffc999bb79a
91ffe6fab7b33ff47b184b59356408951176c670cad3afcde79aa8464374acd3
6f3d4fb64de9ae61776fd19a8eba3d1d828e7e26bb89ace00c7843a57c5f6e8a
e88ea5eb642eaf832f8399d0337ba9eb1563862ddee68c26a74409a7384b9bb9
68f97bf3d03b1733944c25ff4933e4e03d973ccdd73d9528f4d68806b826735e
00ddae5bbc2ddf29954749519ecfb3978a68db6237ebea8e646a898c353053ce
c2ebaf4366835e16f34cc7f0b56f8eaf80a9818375c98672bc678bb4107b4d8c
aa86f4587423c2ff677aebae604614030f9f4d38280409501662ab4e4fe20c2a
fc21814a5f9ed2f6bef9e15b113d00f9291a6553c1e02cc0b4c185c6030eca45
7e031a04e570cddda907d0b4b7af19ce60dc481394dfb3813796ce0e6d079305
0b0e6b40a63710b4f7e6d00d7a4a86e6db2df720fef48640ab6d9d88352a4890
5c7e3cde4d286909154e9a5ee5a5d061a1f0efaa9875fb50c9073e1e8b6cfaef

BBSRAT SHA256 Hashes

567a5b54d6c153cdd2ddd2b084f1f66fc87587dd691cd2ba8e30d689328a673f
cd3b8e4f3a6379dc36fedf96041e292b4195d03f27221167bce7302678fb2540

BBSRAT C2 Servers

jowwln.cocolco[.]com
pagbine.ofhloe[.]com
cdaklle.housejjk[.]com

Cmstar SHA256 Hashes

c3253409cccee20caa7b77312eb89bdbe8920cdb44f3fabfe5e2eeb78023c1b8
3e2c0d60c7677d3ead690b1b6d4d7c5aaa2d218679634ac305ef3d75b5688e6a
3a7348d546d85a179f9d52ff83b20004136ee584993c23a8bfe5c168c00fbaa9
19ba40a7fa332b750c7d93385dd51bd08ee63f91cedb4ae5a93f9f33ecb38c44
4e1d59042336c3758e77c5c521f60ae262aad01bf7265581de54e869a02b65bc

Cmstar C2 Servers

http://thbaw.ofhloe[.]com/cgl-bin/conime.cgi
http://dolimy.celeinkec[.]com/cgl-bin/upl.cgi
http://question.eboregi[.]com
http://pplime.savecarrots[.]com/cgl-bin/upsd.cgi
http://dolimy.celeinkec[.]com/bin/r0206/update.tmp